**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**
**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**
**KHOA VIỄN THÔNG II**

# BÁO CÁO
# ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

**CHUYÊN NGÀNH: ĐIỆN TỬ - TRUYỀN THÔNG**
**HỆ: ĐẠI HỌC CHÍNH QUY**
**NIÊN KHÓA: 2015-2020**

**Đề tài:**

## Ứng dụng Blockchain trong phân phối video

| | |
|---|---|
| **Sinh viên thực hiện:** | **NGUYỄN HOÀI NAM** |
| **MSSV:** | **N15DCVT036** |
| **Lớp:** | **Đ15CQVT01** |
| **Giáo viên hướng dẫn:** | **PGS.TS. VÕ NGUYỄN QUỐC BẢO** |
| | **TS. NGUYỄN VĂN MÙI** |

**Tháng 12 năm 2019**
**TP.HCM - 2019**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**
**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**
**KHOA VIỄN THÔNG II**

# BÁO CÁO
# ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

**CHUYÊN NGÀNH: ĐIỆN TỬ - TRUYỀN THÔNG**
**HỆ: ĐẠI HỌC CHÍNH QUY**
**NIÊN KHÓA: 2015-2020**

**Đề tài:**

## Ứng dụng Blockchain trong phân phối video

NỘI DUNG:

- Chương 1: Tổng quan Blockchain
- Chương 2: Mô hình phân phối video
- Chương 3: Xây dựng mô hình đề xuất trong phân phối video
- Chương 4: Đánh giá mô hình đề xuất

| | |
|---|---|
| **Sinh viên thực hiện:** | **NGUYỄN HOÀI NAM** |
| **MSSV:** | **N15DCVT036** |
| **Lớp:** | **Đ15CQVT01** |
| **Giáo viên hướng dẫn:** | **PGS.TS. VÕ NGUYỄN QUỐC BẢO** |
| | **TS. NGUYỄN VĂN MÙI** |

**Tháng 09 năm 2019**
**TP.HCM - 2019**

# NHẬN XÉT CỦA GIẢNG VIÊN

# LỜI CẢM ƠN

Học tập là quá trình tìm tòi kiến thức và rèn luyện bản thân không ngừng. Trong suốt quá trình học tập và hoàn thành đề tài thực tập, em đã nhận được sự giúp đỡ từ các thầy cô và mọi người xung quanh. Để bày tỏ lòng biết ơn của mình, em xin chân thành gửi lời cảm ơn đến thầy hướng dẫn **PGS.TS. Võ Nguyễn Quốc Bảo** và thầy **TS. Nguyễn Văn Mùi** đã hướng dẫn tận tình, và có những lời đóng góp ý kiến cho đề tài của em.

Em chân thành gửi lời cảm ơn quý thầy cô khoa Viễn Thông 2 đã giúp đỡ em trong quá trình học tập và rèn luyện bản thân trong suốt những năm qua.

Em chân thành gửi lời cảm ơn đến các bạn sinh viên thuộc IoTsLab đã giúp đỡ trong suốt thời gian sinh hoạt tại phòng lab.

Em chân thành gửi lời cảm ơn đến gia đình và bạn bè đã luôn ở bên cạnh và động viên em trong suốt thời gian thực hiện đồ án.

Hồ Chí Minh, ngày 09 tháng 12 năm 2019

Sinh viên thực hiện

**Nguyễn Hoài Nam**

# MỤC LỤC

# THUẬT NGỮ VIẾT TẮT

| Từ Viết Tắt | Tiếng Anh | Tiếng Việt |
|---|---|---|
| PoW | Proof of Work | Bằng chứng công việc |
| VoD | Video-on-demand | Video theo yêu cầu |
| SVOD | Subscription VoD model | |
| TVOD | Transactional VoD model | |
| AVOD | Advertisement-Supported VoD model | |
| CDN | Content Delivery Network | Mạng phân phối nội dung |
| OTT | Over The Top | Giải pháp cung cấp nội dung thông qua Internet |
| IPFS | InterPlanetary File System | Giao thức phân phối ngang hàng |
| DApp | Decentralized Application | Ứng dụng phi tập trung |
| DAG | Directed Acyclic Graphs | Thuật toán sắp xếp topo |
| VCS | Version Control System | Hệ thống quản lý phiên bản phân tán |
| CLI | Command-line interface | Giao diện dòng lệnh |
| ERC-20 | Ethereum Request for Commnent | Chuẩn quy tắc cho smart contract |
| GHOST | Greedy Heaviest Observed Subtree | Giao thức trong Ethereum |
| EVM | Ethereum Virtual Machine | Máy ảo Ethereum |
| IDE | Integrated Development Environment | Môi trường phát triển tích hợp |
| ABI | Application Binary Interface | Giao diện nhị phân ứng dụng |
| HTTP | HyperText Transfer Protocol | Giao thức truyền tải siêu văn bản |
| IPC | Inter Process Communication | Liên lạc giữa các tiến trình |

# DANH SÁCH HÌNH VẼ

# DANH SÁCH BẢNG

# LỜI MỞ ĐẦU

Cách mạng công nghệ 4.0 đã mở ra các xu hướng công nghệ mới như Internet of Things, trí tuệ nhân tạo (AI) hay gần đây nhất là công nghệ Blockchain. Việc ứng dụng các công nghệ mới vào trong cuộc sống sẽ giúp gia tăng sự hiệu quả và cải thiện được những hạn chế của các kỹ thuật hiện có trong cuộc sống của chúng ta.

Với sự phát triển mạnh mẽ của hàng loạt công nghệ mới, xuất hiện ngày nhiều hơn những dịch vụ, nền tảng cung cấp nội dung video. Nổi bật nhất trong lĩnh vực này có thể nhắc đến Youtube hay Netflix, cùng với những cái tên mới nổi như Hulu hoặc là Apple TV. Mặc dù các mô hình phân phối nội dung này đã đi dần vào hoàn thiện nhưng vẫn còn đó là những hạn chế nhất định. Với sự nổi lên đầy hứa hẹn gần đây của công nghệ Blockchain, nổi bật với tính bảo mật và là một nền tảng phi tập trung. Với ý tưởng thông qua những điểm mạnh của mạng Blockchain để phần nào đó khắc phục được những điểm hạn chế trên mô hình phân phối video truyền thống.

Để có cái nhìn tổng quan và cụ thể nhất, trong đề tài này, em sẽ tập trung nghiên cứu mô hình phân phối nội dung video truyền thống, đồng thời tìm hiểu hạn chế trong phương thức hoạt động của mô hình này. Từ đó đề xuất phương hướng cải thiện thông quan những điểm mạnh của Blockchain. Cuối cùng là xây dựng đề xuất và đánh giá kết quả của đề xuất này.

Nội dung đề tài bao gồm 4 chương:

- **Chương 1:** Tổng quan Blockchain
- **Chương 2:** Mô hình phân phối video
- **Chương 3:** Xây dựng mô hình đề xuất trong phân phối video
- **Chương 4:** Đánh giá mô hình đề xuất, phương hướng phát triển

# CHƯƠNG 1

# TỔNG QUAN BLOCKCHAIN

## 1.1 Khái niệm Blockchain

Blockchain[1] được ví như là một cơ sở dữ liệu lưu trữ thông tin trong các khối, các khối này được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Có thể xem blockchain là một sổ cái kỹ thuật số, sổ cái này công khai trong mạng blockchain và lưu lại tất cả các giao dịch. Các giao dịch này được thực hiện và lưu trữ trong các block mà không cần xác nhận bởi bên thứ ba, dữ liệu trong các giao dịch này dường như không thể thay đổi hay chỉnh sửa được.

Blockchain đầu tiên được phát minh và thiết kế bởi Satoshi Nakamoto[2] vào năm 2008 và được hiện thực hóa vào năm sau đó. Với việc sử dụng mạng lưới ngang hàng và một hệ thống dữ liệu phân cấp, blockchain được quản lý tự động trong hệ thống giao dịch mà các thành viên không cần tin tưởng nhau. Trong giai đoạn phát triển đầu tiên, blockchain được thiết kế trong ứng dụng thanh toán, tài chính. Các phiên bản sau này được phát triển với mục đích ứng dụng hiệu quả trong nhiều lĩnh vực hơn.

Trong cùng một nền tảng cốt lõi, tùy theo yêu cầu và đặc điểm ứng dụng blockchainn được chia thành 3 loại phổ biến: public blockchain, private blockchain và consortium blockchain. Trong phạm vi bài báo cáo, public blockchain và private blockchain là hai đối tượng nghiên cứu chính trong mô hình đề xuất và xây dựng.

## 1.2 Các khái niệm liên quan

- Block: Khối là thành phần cơ sở tạo nên chuỗi khối blockchain. Trong mỗi khối gồm có block header và block body, các thông số trong block gồm có:
  - Block version: mang thông tin về phiên bản chứa các thông tin về quyền, quy luật xác thực block vào chuỗi.
  - Merkle tree: giá trị mã băm (hash) của các giao dịch (transaction) trong block.
  - nBit: ngưỡng đích cho quá trình xác thực block.
  - Nonce: một vùng 4 bytes, bắt đầu bằng 0 và tăng lên sau mỗi quá trình tính mã băm.

  - Parent block hash: 256 bits mã băm của khối trước đó.
  - Block body chứa thông tin về các giao dịch, số lượng các giao dịch phụ thuộc vào dung lượng của chúng.

- Smart Contract: hợp đồng thông minh mang thông tin mô tả những điều khoản giữa các bên tham gia. Đảm bảo sự nhanh gọn và minh bạch trong các giao dịch. Hợp đồng thông minh cho phép triển khai giao dịch mà không cần tham gia của bên thứ ba. Những điều khoản này dễ dàng được truy xuất nhưng không thể bị can thiệp. Các bên tham gia vào mạng có thể thực thi các điều khoản trong hợp đồng dưới dạng các câu lệnh trong ngôn ngữ lập trình.

- Proof of Work (PoW): là phương thức đồng thuận trong mạng Blockchain mục đích là xác thực một block mới vào chuỗi. Những node trong mạng tiến hành thay đổi giá trị nonce trong block để lấy những giá trị băm khác nhau. Sự đồng thuận yêu cầu giá trị tính toán nhỏ hơn hoặc bằng một giá trị ngưỡng cho trước. Độ khó (difficulty) sẽ quyết định thời gian tính toán trong tiến trình xác thực block, node sẽ nhận được phần thưởng sau khi xác thực thành công block mới. Node tiến hành xác thực được xem là miner, PoW là hoạt động mining trong blockchain.

- Hash function: là hàm băm biến đổi dữ liệu (ký tự hay số) thành chuỗi được mã hóa theo độ dài cố định, được tạo ra dựa trên thông tin trong block header. Giá trị băm được sử dụng trong các tiến trình tính toán, xác thực chữ ký hay xác thực block mới vào trong chuỗi. Mặt khác, giá trị băm còn giúp cho việc bảo mật được chặt chẽ hơn.

## 1.3 Cơ chế hoạt động

- Smart contract: Smart contract là tập hợp các điều khoản thực hiện một cách tự động. Hợp đồng được soạn bằng ngôn ngữ lập trình, sau đó được mã hóa và chuyển vào một block trong mạng blockchain thông qua tiến trình Proof of Work (PoW), với nền tảng là sổ cái công khai, hợp đồng có thể được truy xuất bởi các node tham gia. Khi có nhận lệnh triển khai hợp đồng sẽ được triển khai theo đúng như điều khoản định sẵn. Đồng thời, Smart contract cũng sẽ tự động kiểm tra quá trình thực hiện những cam kết, điều khoản được nêu trong hợp đồng.

  Các giao dịch đơn giản có thể trực tiếp thực hiện giữa các bên tham gia mà không cần phải thông qua Smart contract. Tuy nhiên, đối với các ứng dụng chuyên biệt có sử dụng

nền tảng blockchain thì Smart contract là một đối tượng cần thiết và quan trọng trong tiến trình ứng dụng. Các node truy xuất vào hợp đồng thông qua địa chỉ sau khi tiến trình xác thực PoW.

- Xác thực giao dịch: Trong tiến trình xác thực Proof of Work, để xác thực khối giao dịch, các node chịu trách nhiệm xác thực phải chứng minh được sự tin cậy sau khi qua nhiều quá trình tính toán. Trong các mô hình khác thì việc lựa chọn node trong xác thực giao dịch sẽ khác nhau (genesis block luôn là block xác thực giao dịch trong private blockchain).

- Nguyên lý mã hóa: Như đã được đề cập, sổ cái được duy trì bởi một nhóm các máy tính được kết nối trong mạng ngang hàng thay vì đưa vào một thực thể tập trung đóng vai trò trung gian. Điều này dẫn đến một số đặc tính khác biệt: mọi người tham gia đều biết được các giao dịch, không yêu cầu sự tin cậy trong các giao dịch.

  Để có thể thực hiện giao dịch trên blockchain, yêu cầu một ví điện tử giúp cho việc lưu trữ trao đổi các đơn vị tiền tệ. Ví này được bảo vệ bằng cặp khóa đặc biệt và duy nhất: khóa riêng tư (private key) và khóa công khai (public key).

  Nếu một thông điệp được mã hóa bằng khóa công khai cụ thể thì chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp. Khi mã hóa một yêu cầu bằng khóa riêng tư từ ví tức là quá trình tạo ra chữ ký điện tử và được các máy tính trong mạng sử dụng để kiểm tra chủ thể và tính xác thực của giao dịch này.

- Quy tắc sổ cái: Mỗi node trong mạng blockchain đều có được bản sao của sổ cái. Do vậy, mỗi node đều biết số dư của một tài khoản nào đó. Hệ thống blockchain không hề theo dõi số dư tài khoản này, mà chỉ ghi lại thông tin của mỗi giao dịch được mỗi khi được diễn ra.

  Sổ cái trên thực tế theo dõi mọi giao dịch được phát đi trong mạng blockchain. Việc xác định số dư này được thực hiện nhờ các tính toán dựa vào liên kết đến các giao dịch trước đó. Trước khi thực hiện một giao dịch, các tính tính toán dựa vào liên kết đến các giao dịch trước đó, các liên kết được xem là giá trị đầu vào, các node trong mạng sẽ xác minh các giá trị này. Để đơn giản và tăng tốc quá trình xác minh, một bản ghi sẽ lưu lại thông tin được node mạng lưu trữ.

  Tất cả nguồn để thực hiện các giao dịch trên mạng blockchain đều là mã nguồn mở. Trong trường hợp có bất kì lỗi nào xảy ra trong quá trình giao dịch, các đơn vị tiền tệ sẽ bị mất đi và không thể khôi phục lại.

- Nguyên lý tạo khối: Các giao dịch sau khi được xác thực trên mạng blockchain sẽ được nhóm vào các khối. Các giao dịch trong cùng một khối được xem là đã xảy ra cùng một lúc và các giao dịch chưa thực hiện trong một khối được coi là chưa xác nhận. Các giao dịch có thể được nhóm lại trong một block và xác nhận vào mạng blockchain như một hàm ý cho các khối tiếp theo được gắn vào sau đó.

  Để được thêm vào blockchain, mỗi khối phải chứa một đoạn mã như là đáp án của một vấn đề toán học được tạo ra bằng hàm băm và không thể đảo ngược. Giải quyết bằng cách đoán các số ngẫu nhiên. Vì trong mạng lưới có nhiều máy tính tập trung việc tìm ra dãy số nên mạng lưới yêu cầu mỗi khối được tạo ra trong khoảng thời gian 10 phút một lần, node nào tìm ra được dãy số trước thì sẽ được quyền gắn khối tiếp theo lên chuỗi và gửi nó đến toàn bộ mạng lưới.

  Vấn đề xảy ra nếu một vấn đề được 2 node giải quyết cùng lúc và các khối được đưa lên mạng lưới cùng lúc. Trong trường hợp này, cả hai khối được gửi lên mạng lưới và mỗi node sẽ xây dựng các khối kế tiếp mà nó nhận được trước tiên, tuy nhiên hệ thống blockchain luôn yêu cầu mỗi node phải xây dựng trên chuỗi khối dài nhất mà nó nhận được.

- Tổ chức xác thực giao dịch trong blockchain: Merkle Tree là một cấu trúc dữ liệu. Được ứng dụng trong cấu trúc blockchain kết hợp với hàm băm (hash) mang chức năng xác thực một giao dịch cụ thể mà không cần phải tải xuống toàn bộ mạng blockchain. Merkle Tree giống như cấu trúc cây nhị phân (binary tree). Thông qua các mã giao dịch và mã băm được cung cấp, cấu trúc có thể xác thực được giao dịch hợp lệ nhờ vào các thuật toán băm sau khi đối chiếu với gốc của Merkle Tree.

- Bảo mật trong blockchain: Nếu có bất kỳ sự bất đồng về khối nào được đại diện sau cùng của chuỗi, điều này sẽ dẫn đến khả năng gian lận. Giao dịch xảy ra trong khối thuộc về đuôi ngắn hơn khi khối tiếp theo được giải quyết, giao dịch đó sẽ trở thành giao dịch chưa xác nhận. Khi bất kỳ sự tấn công nào với mục đích tự tạo ra một chuỗi dài hơn. Kẻ tấn công phải kiểm soát hơn 50% công suất tính toán của toàn bộ mạng. Điều này đồng nghĩa với việc trong một khoảng thời gian ngắn kẻ tấn công xác nhận càng nhiều khối do chính kẻ này tạo ra thì thành công càng cao. Tuy nhiên, điều này là rất khó và hoàn toàn không thể xảy ra được.

## 1.4 Đặc điểm

### 1.4.1 Ưu điểm

Phi tập trung: Không như hệ thống giao dịch tập trung yêu cầu người các bên tham gia phải tin tưởng hệ thống tập trung. Tuy vậy, vấn đề về ngẽn cổ chai sẽ xảy ra tại server trung tâm khi hệ thống quá tải. Trong mạng blockchain thực thể trung tâm sẽ không còn, thay vào đó là mạng ngang hàng. Các giao dịch diễn ra trực tiếp với các bên tham gia với nhau, lúc này không cần sự kiểm soát của server trung tâm. Các giao dịch sẽ sử dụng giao thức đồng thuận để đảm bảo các đặc tính trong mạng phi tập trung.

Sự bất biến: Giao dịch có thể được xác thực nhanh chóng và không được node xác thực tiết lộ. Hầu như không thể xóa hay hoàn tác giao dịch (theo lý thuyết, các giao dịch trong mạng blockchain có thể thay đổi được, tuy nhiên những điều kiện này khó có thể được đáp ứng). Block chứa giao dịch vừa được xác thực sẽ thông báo với các node và có thể được tìm thấy ngay lập tức.

Sự ẩn danh: mỗi người dùng tương tác với blockchain thông qua địa chỉ được tạo, địa chỉ này không tiết lộ thông tin nhận dạng của người dùng. Tuy nhiên, sự ẩn danh này không có trong mạng private blockchain cũng như consortium blockchain. Khi người dùng được nhận dạng rõ ràng theo tên.

Sự bảo mật: Mặc dù có nhiều đặc điểm quan trọng làm nên tính bảo mật trong nền tảng blockchain. Hai tính năng quan trọng nhất là đồng thuận và bất biến. Sự đồng thuận của các node về trạng thái thực của mạng và sự hợp lệ về các giao dịch. Bất biến trong việc ngăn chặn sự thay đổi của các giao dịch đã được xác nhận. Cùng với nhau, hai đặc điểm này tạo nên các khung bảo mật cho dữ liệu trong mạng blockchain.

### 1.4.2 Hạn chế

Blockchain là một công nghệ mới kèm theo đó là một loạt những khái niệm mới kèm theo với những ưu điểm nổi bật mà nó mang đến, bên cạnh đó là những hạn chế nhất định trong xây việc ứng dụng nền tảng này.

Kích thước mạng: blockchain cũng như các hệ thống phân tán khác. Yêu cầu một số lượng lớn các node tham gia, nếu không số lượng không đủ hoặc qui mô của mạng blockchain quá nhỏ thì sẽ không tận dụng được những điểm mạnh của mạng blockchain. Đặc biệt là về tính bảo mật khi càng ít node thì khả năng bị tấn công làm thay đổi thông tin giao dịch càng lớn.

Năng lượng tiêu thụ lớn: năng lượng cần thiết để duy trì sổ cái luôn được cập nhật các giao dịch theo thời gian thực. Khi có một node tham gia vào mạng, cùng thời điểm đó, node này giao tiếp với các node khác. Mặt khác, các node cố gắng thực hiện việc xác nhận giao dịch, mỗi node hoạt động với khả năng chịu lỗi ở mức cao, đảm bảo không bị tắt, các thông tin giao dịch được lưu trữ trên blockchain vẫn còn lưu ngay cả khi không còn sử dụng nữa, đồng thời chuỗi khối này vẫn tiếp tục dài ra và không bao giờ dừng lại. Những hoạt động này tiêu tốn năng lượng lớn hay không gian lưu trữ cho sổ cái, gây rất nhiều lãng phí.

Phiên bản nâng cấp[3] sẽ thay đổi luật của các node được tạo ra, tất cả các node trong mạng cần phải cập nhật để tránh lỗi trong quá trình xác thực giao dịch, thậm chí gián tiếp tạo ra lỗ hổng trong mạng có hai loại:

- Soft fork: các quy tắc trong phiên bản mới được tạo ra chặt chẽ hơn phiên bản cũ.
- Hard fork: các quy tắc trong phiên bản mới được tạo ra lỏng lẽo hơn phiên bản cũ.

Giá trị của các giao dịch: trong trường hợp giao dịch có giá trị thấp thì thời gian chờ xác thực sẽ tăng lên, các node ưu tiên cho các giao dịch có giá trị lớn. Giao dịch có giá trị nhỏ được kém ưu tiên hơn. Điều này gián tiếp làm tăng giá trị của các giao dịch lên đồng thời, thời gian xác thực lại dài ra gây ảnh hưởng rất nhiều đến các ứng dụng liên quan sử dụng nền tảng.

## 1.5 Ứng dụng

Ứng dụng trong giai đoạn phát triển đầu tiên của blockchain có thể dễ dàng biết đến đó là Bitcoin và tiền mã hóa. Tuy nhiên, blockchain giờ đây đang cách mạng hóa các ngành công nghiệp. Với những điểm mạnh nổi trội, blockchain được sử dụng để cải thiện những hạn chế còn tồn tại trước đó trong hệ thống. Một trong các lĩnh vực tiêu biểu với blockchain bao gồm:

Trong lĩnh vực giải trí, Spotify[4] là công ty đã mua lại một công ty khởi nghiệp về blockchain nhằm tích hợp công nghệ này vào mô hình quản lý cở sở dữ liệu phi tập trung đảm bảo cho việc kết nối tốt hơn với các nghệ sĩ và các thỏa thuận cấp phép với các nội dung phát hành trên dịch vụ của Spotify.

D-Tube[5] là một nền tảng video phi tập trung tồn tại trên blockchain đồng nghĩa với việc không có máy chủ trung tâm. Đây là một nền tảng nổi bật với khả năng tự kiếm tiền từ người dùng, không có quảng cáo tuy nhiên không được kiểm duyệt nôi dung. Người sáng tạo nội dung có thể sử dụng dịch vụ và biết chắc rằng dữ liệu của mình được an toàn. Thông tin trong dịch vụ sẽ được chia sẻ ngang hàng.

Trong chuỗi cung ứng, việc nắm rõ tình trạng và điều kiện của sản phẩm từ vật liệu thô đến sản phẩm cuối cùng là điều rất quan trọng. Việc ứng dụng blockchain trong chuỗi cung ứng cho phép minh bạch và hiệu quả trong suốt quá trình tạo ra sản phẩm, đảm bảo được niềm tin từ người sử dụng sản phẩm.

Trong lĩnh vực chăm sóc sức khỏe, blockchain tạo điều kiện thuận lợi trong việc lưu trữ và sử dung hồ sơ bệnh nhân. Thu thập dữ liệu di truyền, tiền sử bệnh án nhằm chủ động hơn trong việc phòng bệnh và điều trị bệnh.

Dịch vụ về tài chính là lĩnh vực khó có thể bỏ qua trong danh sách ứng dụng blockchain. Bằng cách tạo ra những giải pháp thanh toán toàn cầu bằng cách kết nối ngân hàng, nhà cung cấp dịch vụ thanh toán, doanh nghiệp và các giao dịch tài sản kỹ thuật số, cho phép giải quyết ngay tức thì, theo nhu cầu.

# CHƯƠNG 2

# MÔ HÌNH PHÂN PHỐI VIDEO

## 2.1 Các hình thức vận hành video theo yêu cầu

Sự gia tăng nhu cầu giải trí của người dùng về các nội dung video, kèm theo đó là yêu cầu tốc độ cũng như băng thông rộng. Để đáp ứng nhu cầu đó, hệ thống video theo yêu cầu (VOD) đã ra đời.

VOD (Video on demand) là một hệ thống cho phép người dùng có thể lựa chọn và xem nội dung video hay chương trình truyền hình theo đúng ý thích của mỗi cá nhân trên nhiều thiết bị được hỗ trợ như TV, máy tính, máy tính bảng, điện thoại, ... thông qua đường truyền internet.

Trong các dịch vụ ứng dụng VoD hiện nay, có ba hình thức VoD được khai thác phổ biến:

- SVOD (Subscription VoD model): Trong hình thức hoạt động này, người dùng cần thanh toán trước khi sử dụng dịch vụ, trong một khoản thời gian tùy vào nhà quản lý dịch vụ quy định. Tiêu biểu cho mô hình hoạt động này gồm có Netflix[6] hay Amazon Prime[7].

- TVOD (Transactional VOD model): Hình thức cung cấp nội dung đã được mua trước đó. Tùy vào nhu cầu mà người dùng sẽ chi trả: trả tiền để xem hay trả tiền để tải xuống. iTune[7] của Apple hay công ty giải trí WWE[8] sử dụng hình thức hoạt động chiến lược này.

- AVOD (Advertisement-Supported VOD model): Không giống như hai hình thức hoạt động phải trả phí, người dùng trong mô hình quảng cáo này được xem nội dung một cách tự do. Tuy nhiên, nhà quản lý dịch vụ này thu nhập từ nhà quảng cáo do vậy các nội dung này được chèn quảng cáo vào trong nội dung, người dùng buộc phải xem quảng cáo trong lúc xem nội dung. Youtube đang đứng đầu phương thức này với phần lớn lợi nhuận đến từ doanh thu quảng cáo.

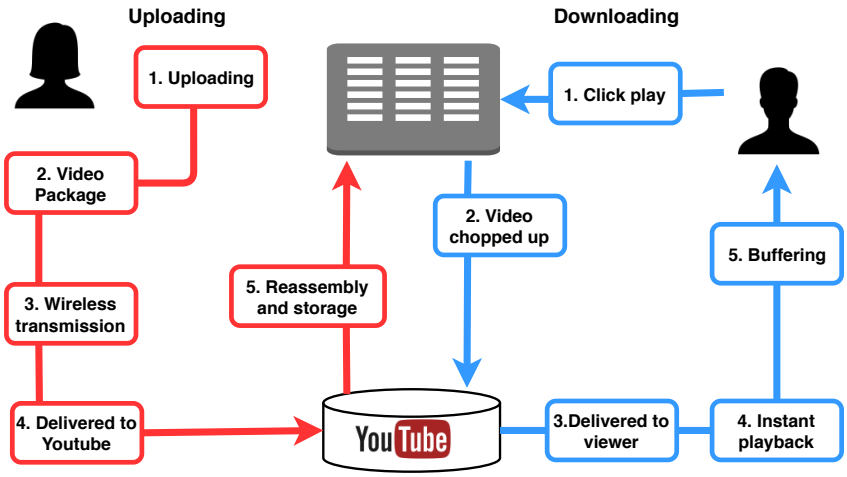
- Hybrid (SVOD + TVOD + AVOD): Mô hình kết hợp các phương thức cung cấp dịch vụ video theo yêu cầu, mang đến nhiều lựa chọn cho người dùng nổi bật với Youtube Premium.

Tại Việt Nam, các hình thức vận hành trên được sử dụng thông qua các nhà cung cấp dịch vụ truyền hình. Người dùng đăng ký gói dịch vụ SVOD thông qua các ứng dụng trên web hay

các ứng dụng di động. Các nhà khai thác dịch vụ tiêu biểu như: SCVT Online, FPT Play. Theo đó, vẫn còn tồn tại dịch vụ truyền hình truyền thống sử dụng đầu thu trong giải mã tín hiệu với sự cải thiện về chất lượng hình ảnh cũng như trải nghiệm người dùng.

## 2.2 Mô hình phân phối video truyền thống

Trong bất cứ hình thức vận hành nào của các dịch vụ cung cấp video đều dựa trên một mô hình phân phối đặc trưng. Trong phạm vi nghiên cứu này, mô hình Youtube được xem là mô hình kiểu mẫu cho các dịch vụ liên quan đến nền tảng phân phối video.




Hình 2.1: Chu trình của video trong mô hình Youtube

Chu trình bắt đầu từ nội dung được người dùng tải lên. Trong một số hình thức dịch vụ khác, nội dung được nhà quản lý tải lên khi đó nhà quản lý trở thành nhà cung cấp đúng nghĩa, không có chức năng chia sẻ nội dung từ người dùng. Người dùng chỉ dừng lại là đối tượng yêu cầu nội dung, không có quyền cung cấp nội dung. Nội dung được đưa lên sau đó được sao lưu ra thành nhiều định dạng khác nhau nhằm tạo ra nhiều mức chất lượng nội dung khác nhau. Đóng gói nội dung. Nội dung sau khi được biến đổi theo mức phân giải sau đó bị chia nhỏ ra nhiều gói nhỏ (packet). Truyền các gói được mã hóa truyền đến server youtube, server này được đặt rải rác nhiều nơi trên thế giới. Tiếp tục được gửi đến trung tâm dữ liệu của Google sau khi liên kết các gói lại với nhau thành một nội dung hoàn chỉnh. Tiến trình tải lên nội dung được hoàn thành.

Tiến trình tiếp theo khi người dùng yêu cầu nội dung từ Youtube thông qua giao diện web. Yêu cầu được gửi đến trung tâm dữ liệu, nội dung từ đây được chia thành nhiều phần nhỏ, lựa chọn định dạng phù hợp cho trình duyệt sau đó gửi đến Youtube server thông qua internet. Youtube server chịu trách nhiệm biến đổi, lựa chọn chất lượng nội dung phù hợp gửi đến thiết

bị người dùng, tùy vào kết nối Internet các gói dữ liệu sẽ được lưu vào trong bộ đệm đợi các gói dữ liệu nội dung được gửi đến lần lượt.

Youtube không dừng lại ở việc chỉ cung cấp dịch vụ video, họ còn mở rộng các dịch vụ liên quan về đặc quyền người dùng hay thu tiền từ những tính năng đặc biệt nhằm cải thiện trải nghiệm người dùng.

### Đặc điểm

**Điểm mạnh**: Việc thay đổi định dạng phù hợp cho từng đối tượng nội dung giúp phù hợp hơn với các nền tảng trình duyệt, điều này giúp người dùng không gặp phải lỗi khi yêu cầu các nội dung video trên nền tảng này. Nội dung được đưa đến trình duyệt một cách tuần tự thông qua bộ đệm giúp đảm bảo nội dung được đáp ứng cho người dùng một cách kịp thời. Do có thời gian hình thành và phát triển lâu dài, những tính năng kèm theo đó khiến người dùng cảm thấy được tăng cảm giác trải nghiệm hơn. Youtube đã tích hợp trí tuệ nhân tạo[9] trong việc gợi ý nội dung, sắp xếp tổng hợp các danh sách phát có liên quan đến lịch sử yêu cầu trước đó. Tùy vào từng đối tượng phục vụ mà các nền tảng cụ thể có những tính năng đặc trưng của họ. Youtube đã giữ chân khách hàng của mình rất tốt trong bối cảnh các nền tảng công nghệ mới với những tính năng nổi trội hơn sẵn sàng làm hài lòng người dùng.

**Hạn chế**: Trong hoạt động, nội dung sau khi đến được thiết bị người dùng phải qua nhiều tiến trình. Mặc dù quá nhiều tiến trình trong mô hình. Nhìn chung, trung tâm dữ liệu - nơi chứa nội dung tập trung và server Youtube chịu trách nhiệm mang chuyển tiếp và tập hợp các thông thành phần của nội dung. Điều này gây nên nhiều rủi ro trong quá trình vận hành. Thứ nhất, vấn đề xử lý tập trung gây quá tải cho server lưu trữ, yêu cầu lưu lượng dữ liệu lớn, băng thông rộng khi phải giải quyết quá nhiều yêu cầu từ người dùng. Thứ hai, trong trường hợp server hoặc trung tâm dữ liệu ngừng hoạt động, nội dung sẽ không thể đến với người dùng hoặc sẽ thông qua một server ở xa hơn tăng thời gian phản hồi trong tiến trình vận hành dịch vụ.

Một vấn đề khác là băng thông. Trường hợp một số lượng lớn người xem cùng một nội dung và cần phải sao lưu nội dung này, khi đó số lượng băng thông yêu cầu tăng lên cùng với số người có nhu cầu xem. Youtube đã giải quyết vấn đề này bằng cách phải tốn thêm chi phí vào xây dựng hệ thống CDN (mạng phân phối nội dung) nhằm tạo ra nhiều máy chủ chứa bản sao nội dung. Mục đích là tối ưu hóa băng thông và giảm thời gian phản hồi. Giải pháp chỉ mang tính tạm thời, khi mà yêu cầu nội dung từ người dùng ngày càng tăng thì giải pháp bổ sung phần cứng trong mô hình sẽ không còn hiệu quả nữa.

Mặt khác, nội dung gốc được tải lên Youtube sẽ bị thay đổi định dạng cho phù hợp. Vì youtube chủ yếu sử dụng hình thức AVOD các nội dung sẽ được nhúng quảng cáo. Dịch vụ của youtube sẽ mất đi tính toàn vẹn đối với nội dung.

Về vấn đề chi phí, người đóng góp nội dung sẽ được lợi nhuận theo phần trăm. Tuy nhiên con số này là rất thấp. Sự khác nhau về lợi nhuận còn khác nhau tùy vào mỗi khu vực trên thế giới.

Người dùng sẽ không nhận được lợi nhuận xứng đáng khi tham gia nền tảng với 45% được nhận từ nhà quảng cáo.

## 2.3 Mô hình phân phối video trong nước

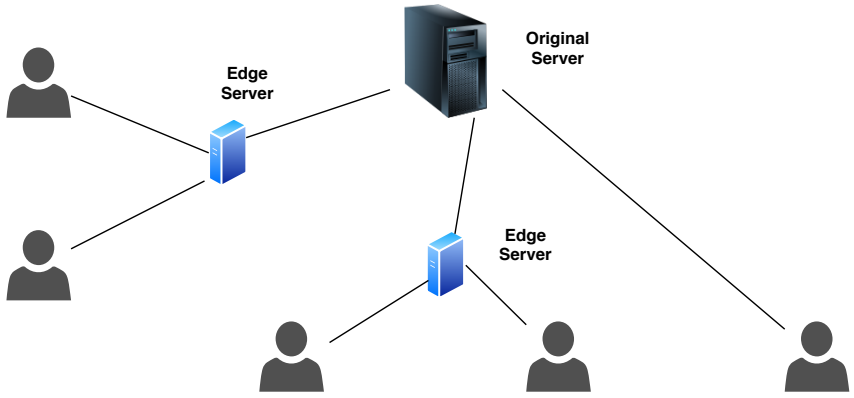
Ở Việt Nam, hình thức kinh doanh video theo yêu cầu (VoD) là một loại hình dịch vụ tiềm năng và khá mới mẻ thời gian gần đây. Các đơn vị kinh doanh cung cấp và phân phối dịch vụ bao gồm clip tv, Galaxy, BHD, cho đến các công ty công nghệ như VNG (Zing TV) hay các đơn vị kinh doanh dịch vụ truyền hình cũng tham gia có SCTV, VTV cab hay FPT. Với tầm nhìn trong tương lai, xu hướng cung cấp nội dung theo yêu cầu thông qua Internet (OTT) sẽ trở thành tất yếu trong tương lai. Hình thức cung cấp chủ yếu ở thị trường Việt Nam chủ yếu là SVOD - đăng ký gói thuê bao, tuy nhiên các gói này được phân loại bằng cách kết hợp với các hình thức vận hành khác như TVOD hay AVOD.

Tuy thị trường cung cấp dịch vụ video theo yêu cầu ở Việt Nam đầy tiềm năng, dự đoán sẽ còn phát triển thêm trong tương lai. Nhưng về mặt kỹ thuật, mô hình được xây dựng để vận hành dịch vụ vẫn còn dùng kiểu quản lý tập trung. Nguyên nhân có thể thấy được từ 2 lý do:

- Mặc dù khái niệm video theo yêu cầu đã có từ lâu, tuy nhiên hình thức kinh doanh này mới thực sự được quan tâm gần đây bởi các nhà cung cấp, phân phối nội dung.
- Tại Việt Nam đầu tiên blockchain được chú trọng đầu tư với mục đích đào tiền ảo (Bitcoin). Khi được tạo ra để hỗ trợ trong các ứng dụng, một nền tảng khác của blockchain là Ethereum, lúc này giải pháp mới xuất hiện giải quyết vấn đề được cho ứng dụng phi tập trung, phân phối video theo yêu cầu là một trong số đó.

Hiện tại, không nhiều các nhà cung cấp dịch vụ video theo yêu cầu sử dụng mô hình quản lý phi tập trung đúng nghĩa. Với SCVT là công ty dịch vụ truyền hình cáp ngoài việc cung cấp các dịch vụ liên quan đến truyền hình, Internet còn vận hành thêm dịch vụ cung cấp video theo yêu cầu. Bằng cách sử dụng server quản lý tập trung các nội dung tải lên phục vụ người dùng. Sử dụng mạng phân phối nội dung CDN trong giải quyết vấn đề về tốc độ và sự quá tải tại server trung tâm Figure 2.2 tương tự như giải pháp được dùng trong các nền tảng khác.

Nhằm đơn giản quy trình cũng như việc vận hành cả mô hình phức tạp, dịch vụ Wowza[10] được sử dụng như là một máy chủ trong việc xây dựng và phân phối các dòng tín hiệu hình ảnh,

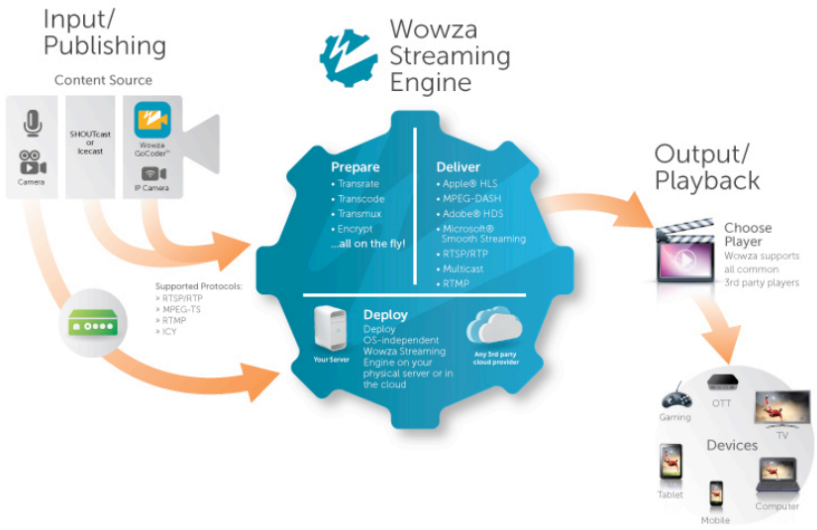



Hình 2.2: Mạng phân phối nội dung

âm thanh đến các thiết bị di động nào của người dùng. Ở Wowza hỗ trợ các dịch vụ liên quan đến streaming video và phân phối video theo yêu cầu trên 2 hình thức: đám mây và phần cứng.

Quy trình hoạt động gồm 3 bước:

- Nội dung video được mã hóa, đóng gói đưa vào Wowza Engine.
- Dữ liệu được đóng gói và đẩy luồng video nén đến Wowza streaming engine
- Tùy ngõ ra với các định dạng khác nhau tùy theo yêu cầu của thiết bị nơi yêu cầu nội dung, mặt khác ngõ ra có thể được dẫn thẳng đến các mạng phân phối nội dung. Nhà quản lý dịch vụ sẽ kiểm soát ngõ ra này theo tùy mục đích rồi mới đến với người dùng




Hình 2.3: Các giai đoạn làm việc của Wowza[11]

Về bản chất, Wowza là một dịch vụ hỗ trợ streaming và phân phối video. Dịch vụ giải quyết được những yêu cầu phức tạp của việc xây dựng hệ thống hay những vấn đề mà các mô hình dịch vụ video theo yêu cầu gặp phải. Vẫn còn đó là xây dựng server tập trung.

Điểm mạnh của việc sử dụng thêm các dịch vụ bên thứ 3 để giải quyết một phần các tiến trình trong ứng dụng một phần đảm bảo cho server hoạt động ổn định trong, các vấn đề liên quan đến băng thông, tốc độ hay bảo mật nội dung đã được bên thứ ba này tham giải quyết, phần còn lại của doanh nghiệp khai thác khá nhẹ nhàng trong việc đưa nội dung đến người dùng. Bên cạnh đó, vấn việc tin tưởng một bên hay để một thành phần khác quản lý server cũng là rủi ro của cả một dịch vụ.

Các doanh nghiệp khác ở Việt Nam chủ yếu vẫn xây dựng trên mô hình truyền thống với server quản lý tập trung giống như mô hình của Youtube đã đề cập tuy nhiên vẫn chưa được ổn định thì việc thay đổi mô hình sẽ là chuyện rất lâu nữa. Ứng dụng server trong quản lý phi tập trung được ứng dụng cho website nhiều hơn mà chưa tập trung vào các dịch vụ liên quan đến video theo yêu cầu.

Các dịch vụ video theo yêu cầu tại Việt Nam đa phần là từ một phía nhà cung cấp. Nhà cung cấp dịch vụ đồng thời cũng là người kiểm duyệt các nội dung dựa theo các quy định của pháp luật cụ thể là luật pháp Việt Nam. Các vấn đề liên quan có thể xảy ra do nhà cung cấp chịu trách nhiệm.

Với tiềm năng có được từ dịch vụ video theo yêu cầu tại Việt Nam, dịch vụ sẽ trở nên mạnh mẽ hơn, thu hút được nhiều người dùng hơn. Và một điều tất yếu khi có nhiều người sử dụng là buộc phải thay đổi cho phù hợp, lúc này mô hình quản lý phi tập trung là lựa chọn phù hợp đáp ứng được cho bài toán tương lai này.

### Đặc điểm

Với sự tiện lợi trong việc đáp ứng kịp thời yêu cầu của người dùng dịch vụ video theo yêu cầu (VoD) hứa hẹn sẽ phát triển rất nhiều trong tương lai. Dần dần cần phải cải tiến để thay đổi, tăng cường trải nghiệm người dùng dịch vụ.

Dù gặp nhiều khó khăn về thói quen người dùng vẫn còn tồn tại nhiều trang web không chính thống, cung cấp nội dung không có bản quyền, gây thiệt hại cho các doanh nghiệp cung cấp nội dung nguyên nhân ở vấn đề bảo mật trong mô hình. Mặt khác luật pháp Việt Nam trong xử lý các vấn đề bản quyền, chưa đủ mạnh, chỉ mang tính răn đe để bảo vệ các nhà cung cấp nội dung có bản quyền. Song với đó, cơ quan nhà nước đang hỗ trợ và tập trung rất mạnh vào việc xử lý dần các dịch vụ vi phạm, đồng thời ý thức người xem ngày một nâng cao, dịch vụ và sản phẩm của các công ty cung cấp có bản quyền ngày một tốt hơn thì việc đầu tư vào bản quyền là một sự đầu tư cho tương lai.

## 2.4 Mô hình đã triển khai

Với những hạn chế trong mô hình truyền thống trong dịch vụ phân phối nội dung. DTube[5] ra đời với mục giải quyết những hạn chế trên trên nền tảng công nghệ mới - blockchain cho ứng dụng phi tập trung. Những tính năng nổi trội lại vừa tiện ích tập trung vào đối tượng tham gia vào ứng dụng. Với DTube người sáng tạo nội dung có thể sử dụng dịch vụ và biết chắc rằng dữ liệu của mình an toàn. Hơn nữa, nội dung không thể bị kiểm duyệt bởi bất kì ai ngoài cộng đồng DTube.

Một loạt đặc tính nổi bật DTube mang đến cho người dùng:

- DTube đã đưa ra những sự thay đổi to lớn bằng cách cho phép người dùng tải lên nội dung thông qua nội dung đã tồn tại trên website, người dùng dễ dàng tải lên nội dung bằng URL. Thay vì nội dung tải lên phải ở dạng tệp, theo format yêu cầu. Nội dung được biến đổi và gửi đến nút IPFS của DTube. Việc tải lên nội dung bị xếp vào hàng đợi quá nhiều.

- DTube không sử dụng máy chủ trung tâm, các tiến trình diễn ra trên mạng blockchain. Về bản chất, dữ liệu trên blockchain được xác minh giữa tất cả các thành viên tham gia vào cộng đồng.

  Các video phi tập trung đồng nghĩa sẽ không có cách đơn giản nào để loại bỏ nội dung khỏi trang web. Điều này có thể là điều tốt hoặc xấu, tùy từng trường hợp cụ thể. Tuy nhiên, đối với một số người dùng, việc đảm bảo rằng nội dung của họ không chịu sự kiểm soát của một tổ chức nào đó là một ưu điểm lớn và là lý do chính đáng để cân nhắc việc chuyển sang DTube.

- DTube không có thuật toán ẩn, các tiến trình diễn ra rõ ràng và tường minh. Dữ liệu người dùng không được lưu trữ ở một nơi duy nhất làm nguy cơ bị tấn công khó xảy ra. Mọi người dùng đăng tải nội dung dưới bút danh, trang web không có thông tin đăng nhập như truyền thống. Thông tin người dùng không muốn chia sẻ không bị rò rỉ ra ngoài. Bản quyền nội dung được bảo mật tốt hơn, phần nào chủ động trong việc hạn chế việc khai thác nội dung không chính thống.

- Không còn tồn tại hình thức quảng cáo AVOD như truyền thống. Người dùng bầu chọn nội dung để nhận được tiền. Đơn vị tiền tệ trong nền tảng này là STEEM dollar. Người tạo nội dung có thể tự tạo quảng cáo cho nội dung của mình, thông qua STEEM bằng cách bầu chọn nội dung người dùng có thể kiếm tiền thông qua dịch vụ này.

- Không chịu bất kì sự kiểm duyệt nào tạo nên một môi trường tự do về nội dung. Cộng đồng tự đánh giá tất cả nội dung, về nguyên tắc nền tảng cho phép nội dung xuất hiện trên website, trên thực tế cộng đồng hoạt động khá tốt trong việc lọc ra những nội dung không có giá trị hay mang tính nguy hiểm. Vấn đề này có thể tốt hoặc xấu, tùy vào quan điểm của người dùng.

- DTube hoạt động độc lập với các dịch vụ đến từ các tập đoàn công nghệ lớn như Google hay Facebook. Do là một phần của cuộc cách mạng blockchain, DTube được xem là tiên phong trong việc tìm ra cách mới để chia sẻ các nội dung sáng tạo và phong phú.

Không dừng lại ở đó, trên thể giới không ít các dự án về xây dựng mô hình dịch vụ cung cấp nội dung trên nền tảng blockchain.

- MovieCoin: Dựa trên nền tảng blockchain, cho phép đầu vào các dự án phim ảnh. Hình thức đầu tư thông qua đơn vị tiền tệ riêng của công ty này. Người dùng trả tiền này để thuê phim trực tiếp từ studio mà không phải tốn chi phí cho đơn vị trung gian.

- White Rabbit: Một ứng dung khác xây dựng trên nền tảng blockchain, cho phép người dùng kiếm tiền ngay trên các nội dung của chính họ.

- Dự án của nhóm nghiên cứu trường đại học Khalifa, UAE[12]. Đề cập đến dịch vụ cung cấp các dịch vụ về ebook nhằm đảm bảo quyền tác giả trong các giao dịch thông qua IPFS và blockchain.

## 2.5 Mô hình đề xuất

Mô hình phân phối nội dung gồm ba khối chức năng chính:

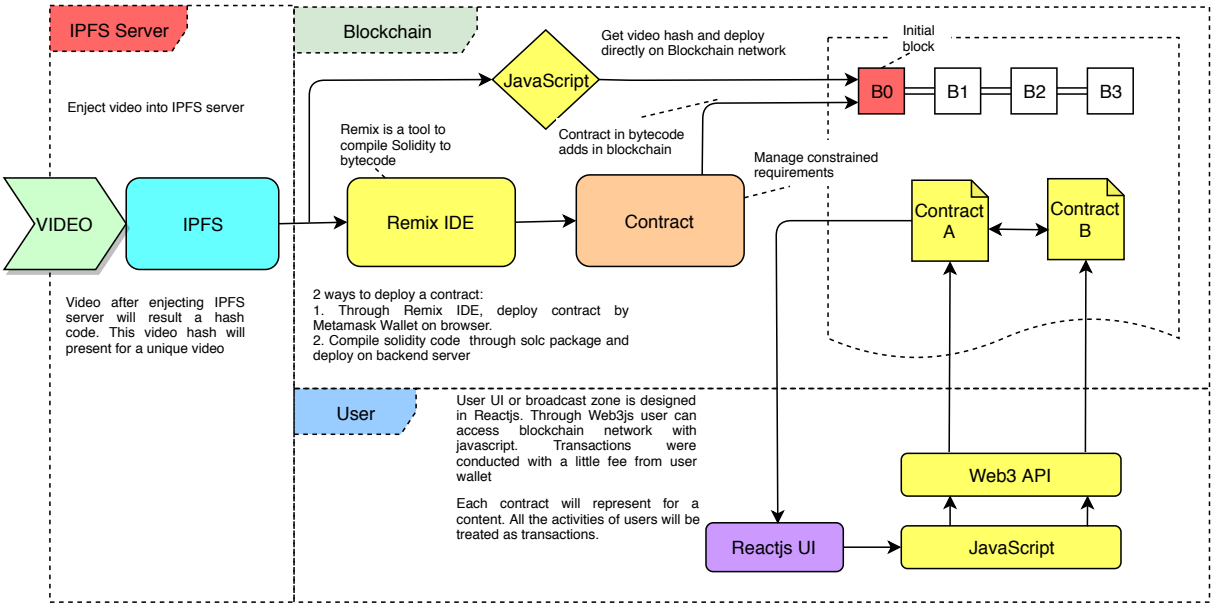
- Khối xử lý nội dung tải lên

- Khối vận hành, phân phối nội dung

- Khối tương tác người dùng

Những vấn đề gặp phải trong mô hình truyền thống phần lớn được giải quyết bởi mô hình đề xuất này.

- Khối xử lý nội dung tải lên: Với mô hình tập trung, dữ liệu video qua các bước xử lý sẽ được đưa lên server rồi đến trung tâm dữ liệu (Data center) theo chiều tải lên của nội




Hình 2.4: Mô hình phân phối video đề xuất

dung. Trong khi thông qua IPFS nội dung không cần thêm bước xử lý nào trước đó mà trực tiếp đưa nội dung lên server phi tập trung. Việc truy xuất nội dung đã được đưa lên IPFS server chỉ là yêu cầu từ các nút (peer) tham gia. Server hay trung tâm dữ liệu bây giờ sẽ không cần thiết. Khi IPFS đã cơ bản thay thế được trong vấn đề lưu trữ nội dung nhờ vào cơ chế lưu trữ nội dung trên các nút tham gia vào mạng IPFS. Với sự gia tăng số lượng người dùng trong tương lai, mô hình IPFS sẽ càng hiệu quả hơn do số lượng nút lưu trữ tăng lên. Tiết kiệm chi phí cho lưu trữ là một điểm lợi lớn.

- Khối vận hành, phân phối nội dung: Người dùng truy xuất vào mạng Blockchain và tham gia như là một người dùng để tương tác với nội dung. Mỗi nội dung được quản lý bởi một hợp đồng riêng biệt điều này hạn chế được rủi ro mất mát nội dung trường hợp không thể xác thực hợp đồng. Mạng blockchain đóng vai trò trung gian, là mạng phi tập trung thứ hai trong mô hình đảm nhận việc quản lý người dùng và phân phối nội dung yêu cầu trong khuôn khổ một nội dung, người dùng sẽ được quản lý trong một bản hợp đồng chứa nội dung đảm bảo không xảy việc chia sẻ nội dung khi chưa trả phí. Blockchain sẽ dẫn người dùng trực tiếp đến nội dung yêu cầu thay thế được chức năng định tuyến nội dung trong mô hình cũ.

- Khối tương tác người dùng: Là một ứng dụng phi tập trung (DApp) hạn chế được vấn đề kiểm duyệt cũng như là máy chủ. Số lượng người dùng truy cập vào một DApp tại cùng một thời điểm không còn là vấn đề nhờ vào tính phi tập trung của nền tảng.

Có thể thấy rằng có hai mạng phi tập trung được sử dụng trong mô hình, gồm: IPFS, và

mạng Blockchain. Hai mạng phi tập trung này giải quyết được hai tiến trình trong dịch vụ, là phương tiện lưu trữ, mặt khác là phương tiện định tuyến tìm đến các nội dung. Hai tiến trình quan trọng này sẵn sàng thay thế những bước phức tạp đồng thời là các hạn chế của của mô hình truyền thống.

Nội dung tải lên sẽ được biến đổi thành một chuỗi băm thông qua giao thức IPFS[13]. Giải quyết được vấn đề phải thông qua nhiều bước biến đổi trong mô hình truyền thống. Nội dung sẽ không còn lưu trữ ở trung tâm dữ liệu, tránh được sự phân bố tập trung. Đồng thời, nội dung chỉ được nhà quản lý biết được nên việc nội dung bị tấn công là rất khó xảy ra.

Lúc này nội dung được đại diện bởi một chuỗi băm, thông qua chuỗi này được đưa vào smart contract sau đó là xây dựng và xác thực trên mạng blockchain. Chuỗi địa chỉ đại diện cho smart contract chứa nội dung được công khai đến các phần tử trong mạng blockchain. Từ đây, người dùng tham gia vào mạng có thể yêu cầu được nội dung thông qua smart contract.

Hợp đồng thông minh chứa nội dung sau khi được xác thực trên blockchain được quảng bá trên giao diện của một ứng dụng DApp (Decentralzed Application). Người dùng tham gia vào blockchain với các yêu cầu liên quan đến nội dung đều thông qua ứng dụng này.

# CHƯƠNG 3

# XÂY DỰNG MÔ HÌNH ĐỀ XUẤT TRONG PHÂN PHỐI VIDEO

## 3.1 Khối xử lý nội dung tải lên

Trong khối xử lý nội dung tải lên, giao thức IPFS được sử dụng trong cho chức năng biến đổi và lưu trữ nội dung.

Giao thức IPFS[13] (InterPlanetary File System) là giao thức cho phép chia sẻ các tập tin ngang hàng với nhau mà không cần sự có mặt của máy chủ trung tâm. Mỗi nội dung được tải lên sẽ nhận được chuỗi băm (hash), các nội dung giống nhau sẽ có mã băm giống nhau, từ đây loại bỏ được sự trùng lặp. Nội dung sau khi được đưa lên bị chia thành nhiều phần nhỏ và được lưu trữ ở các node khác. Trường hợp, khi muốn tải về một tập tin, một nút sẽ yêu cầu máy chủ tìm trong một bảng băm phân tán có thông tin của tất cả mọi nút trong mạng để tìm ra được các mảnh của nội dung được lưu trữ ở những nút nào, công cuộc tìm kiếm được thực hiện một cách hiệu quả thông qua các mô đun mang từng chức năng riêng biệt tham gia vào hệ thống.

IPFS là một mạng ngang hàng, dữ liệu được chứa trong mạng local, các nút trong mạng liên kết và trao đổi dữ liệu với nhau. Giao thức IPFS được chia thành chồng các giao thức với chức năng riêng biệt:

- Nhận dạng (Identities): nút được nhận dạng bởi NodeId - là mã băm được mã hóa. Có vai trò kiểm soát khởi tạo nhận dạng và xác thực nút.
- Mạng (Network): kết nối đến các nút khác thông qua các giao thức kết nối và chuyển vận, với các tùy chọn trong nền tảng.
- Định tuyến (Routing): IPFS yêu cầu tìm đến các nút khác hay các nút liên quan đến nội dung yêu cầu.
- Trao đổi (Exchange): giao thức trao đổi nút mới quản lý việc phân tán khối hiệu quả hơn.
- Đối tượng (Object): gồm phần dữ liệu và mảng chứa liên kết đến các node chứa phần dữ liệu còn lại.

- Tập tin (Files): tập hợp các đối tượng lại với nhau trong IPFS.
- Tên (Name): tên đối tượng trong IPFS và không thể thay đổi được .

Đối tượng làm việc chính trong giao thức IPFS là tập tin. Cấu trúc tập tin trong IPFS là cấu trúc Merkle DAG được kết hợp từ Merkle tree sử dụng trong blockchain để đảm bảo tính toàn vẹn của các giao dịch. Song với đó là Directed Acyclic Graphs (DAG) được sử dụng trong công cụ Git[14].

Để hỗ trợ khả năng trong việc ghi nhận sự thay đổi nội dung của các đối tượng tập tin tại nơi lưu trữ (repository). DAG được sử dụng trong việc cấu trúc những thay đổi này của các đối tượng trong repository. Ghi lại lịch sử thay đổi trong nơi lưu trữ thành một chuỗi.

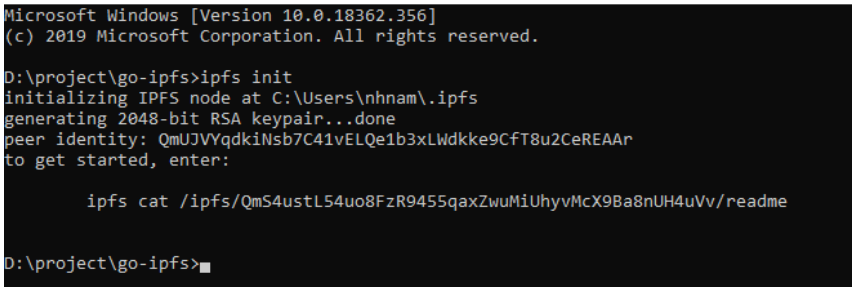
Có 3 vấn đề quan trọng của tiến trình trong IPFS:

- IPFS sử dụng địa chỉ để nhận dạng nội dung. Mỗi phần của nội dung đều sử dụng giao thức nhận dạng của IPFS hay là CID, chúng đều là một chuỗi băm. Chuỗi băm là duy nhất cho một nội dung. Địa chỉ của nội dung thông qua chuỗi hash được sử dụng rộng rãi trong cơ chế kết nối của nhiều hệ thống phân tán. Nội dung được nhận diện sau đó được IPLD dịch ra cấu trúc dữ liệu phù hợp cho từng hệ thống.
- IPFS cũng như các hệ thống khác sừ dụng cấu trúc Merkle DAG trong việc đảm bảo cho sự hiện diện của các tệp và thư mục, cùng với đó là sao lưu những nội dung đi đến các nút.
- DHT (Distributed Hash Table): Để tìm được nút nào đang chứa nội dung cần truy xuất thông qua bảng băm (hash table). Bảng này chứa một khóa trỏ đến một giá trị. Khi biết được vị trí của nội dung, bảng băm lại được sử dụng để truy ra vị trí của nút đó. Để yêu cầu khối và gửi khối đến các nút khác. Mô đun Bitswap được dùng để kết nối một nút đến các nút khác mang nội dung yêu cầu, bổ sung vào danh sách yêu cầu và khối được gửi đến. Khối gửi đến được xác thực bằng CID.

Trong phạm vi nghiên cứu, nội dung được đưa lên IPFS trước khi được chuyển tiếp vào hợp đồng (smart contract) thuộc khối blockchain, sẽ được đề cập trong phần tiếp theo của chương. Mô hình xây dựng trong kiểm thử bắt đầu từ việc tương tác người dùng với nội dung trong bản hợp đồng thông minh (smart contract), bắt đầu từ chức năng tải lên đến việc tương tác nội dung cũng như tính năng thu lợi nhuân từ nội dung tải lên trong phạm vi xây dựng mô hình.

Nội dung trước khi được đưa lên IPFS, yêu cầu trước tiên máy tính phải là một nút (peer) có thể xem đây là thủ tục đầu tiên để tham gia vào mạng. Để trở thành một người dùng tham gia

vào hệ thống IPFS, cần phải cài đặt vào máy tính. Người dùng tương tác với mạng thông qua cửa sổ lệnh CLI.




Hình 3.1: Khởi tạo nút tham gia vào IPFS

Lệnh `ipfs init` khởi tạo nút tham gia vào mạng, sau khi khởi tạo, hệ thống trả về địa chỉ nơi lưu các tệp, địa chỉ nhận dạng nút, mỗi máy tính đều có địa chỉ nhận dạng này. Các nút có thể liên kết hay trao đổi dữ liệu trực tiếp với nhau thông qua địa chỉ nhận dạng này. Trong hình 3.1 nút có địa chỉ `QmUJVYqdkiNsb7C41vELQe1b3xLWdkke9CfT8u2CeREAAr`, địa chỉ có độ dài 46 bits, sử dụng mã băm SHA-265 bắt đầu với hai ký tự "`Qm`". Cũng giống như chuỗi băm địa chỉ nút, mã băm của dữ liệu sau khi được đưa lên IPFS đều có dạng tương tự. Trong quá trình vận hành, các tiến trình biến đổi hay nhận dạng đều lấy chuỗi băm làm cơ sở.

Thuật toán băm SHA-256[15] có thể xem là thuật toán chính, sử dụng nhiều trong các tiến trình thuộc giao thức IPFS. Mặt khác, thuật toán này còn là kỹ thuật chính trong cấu trúc lõi của hệ sinh thái blockchain. Với khả năng biến đổi một chuỗi đầu vào thành một chuỗi đầu ra với độ dài cố định. Mỗi chuỗi đầu vào duy nhất cho ra một chuỗi đầu ra duy nhất, và không thể biến đổi ngược lại.

SHA-256 nhận dữ liệu đầu vào có kích thước không vượt quá $2^{64}$ đồng thời ngõ ra có kích thước 32 bits. Dữ liệu phải trải qua 64 vòng tính toán trong tiến trình xử lý đầu ra.

Quá trình xử lý mã băm gồm 3 tiến trình:

- Tiền xử lý: Là bước đầu tiên cho việc khởi tạo các bước xử lý cần cho tiến trình sắp xếp và nén có thể được tiến hành. Tiền xử lý gồm 3 công việc:
  - Bổ sung thêm các bit cần thiết cho dữ liệu vào thỏa mãn là bội của 512.

$$l + 1 + k = 448 \; mod \; 512 \tag{3.1}$$

Với $l$ là độ dài của dữ liệu vào, $k$ là số nguyên dương nhỏ nhất để đạt giá trị thỏa mãn thỏa mãn đồng dư với 448 (mode 512).

  - Phân tích thành các khối 512 bits: sau khi được bổ sung các bits vào dữ liệu gốc, từ đây được phân tích thành các khối 512 bits chuẩn bị cho việc sắp xếp và băm dữ liệu.
  - Khởi tạo giá trị băm: giá trị khởi tạo này được tạo ra bằng cách lấy 32 bit đầu tiên của phần phân số của căn bậc 2 của 8 số nguyên tố đầu tiên.

- Sắp xếp dữ liệu: Sau quá trình tiền xử lý, khối sắp xếp dữ liệu vào sẽ lấy khối 512 bits đầu tiên với ngõ ra dữ liệu phụ thuộc vào mỗi vòng lặp từ giá trị $W_0$ đến $W_{63}$, và được chia làm 2 chặng như biểu diễn:

$$
\begin{aligned}
&for\ 0 \leq t \leq 15, \\
&W_t = M_t \\
&for\ 16 \leq t \leq 63, \\
&W_t = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-5}) + W_{t-16}
\end{aligned} \tag{3.2}
$$

  Với, $\sigma_0$ và $\sigma_1$ là hai hàm logic đặc trưng cho hàm băm dữ liệu sắp xếp dạng SHA-256 được triển khai trên 32 bit được minh họa như sau:

$$\sigma_0 = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \tag{3.3}$$

$$\sigma_1 = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \tag{3.4}$$

  Với, $ROTR^x$ là xoay vòng phải x bit, $SHR^x$ dịch phải x bit.

- Hàm nén: Hàm nén dữ liệu hoạt động theo tiến trình băm với yêu cầu bắt buộc phải theo 1 chiều. $W_t$ là giá trị mang 32 bits dữ liệu được tính toán bởi việc sắp dữ liệu đồng thời là ngõ vào cho hàm nén, trong đó $K_t$ là giá trị hằng, SHA-256 sử dụng 64 giá trị hằng số cho mỗi lần chạy, giá trị này là 32 bit đầu tiên của phần phân số của căn bậc 3 của 64 số nguyên tố đầu tiên. Trong quá trình nén, hàm sử dụng 8 ký tự lần lượt là A, B, C, D, E, F, G và H trong cập nhật từng vòng lặp. Giá trị A và E phụ thuộc vào tất cả dữ liệu ngõ vào và được tính bằng công thức ở mỗi vòng. Sau 8 biến làm việc được khởi tạo, 64 vòng lặp của hàm nén được đưa vào công thức và giá trị ở những vòng ở giữa của các biến được

tính theo công thức:

$$T_1 = H + \sum\nolimits_1(\mathrm{E}) + Ch(E,F,G) + K_t + W_t \tag{3.5}$$

$$T_2 = \sum\nolimits_0(\mathrm{E}) + Maj(A,B,C) \tag{3.6}$$

$$H = G; G = F; F = E \tag{3.7}$$

$$E = D + T_1 = D + H + \sum\nolimits_1(\mathrm{E}) + Ch(E,F,G) + K_t + W_t \tag{3.8}$$

$$D = C; C = B; B = A \tag{3.9}$$

$$A = T_1 + T_2 = H + \sum\nolimits_0(\mathrm{E}) + Maj(A,B,C) + \sum\nolimits_1(\mathrm{E}) + Ch(E,F,G) + K_t + W_t \tag{3.10}$$

Các hàm nén ở trên được là cốt lõi của tiến trình. Sau khi thực thi xong các lệnh logic sau 64 vòng lặp.

$$Ch(X,Y,Z) = (X \wedge Y) \oplus \neg(X \wedge Y) \tag{3.11}$$

$$Maj(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z) \tag{3.12}$$

$$\sum\nolimits_0(\mathrm{X}) = ROTR^2(X) \oplus ROTR^{13}(X) ROTR^{22}(X) \tag{3.13}$$

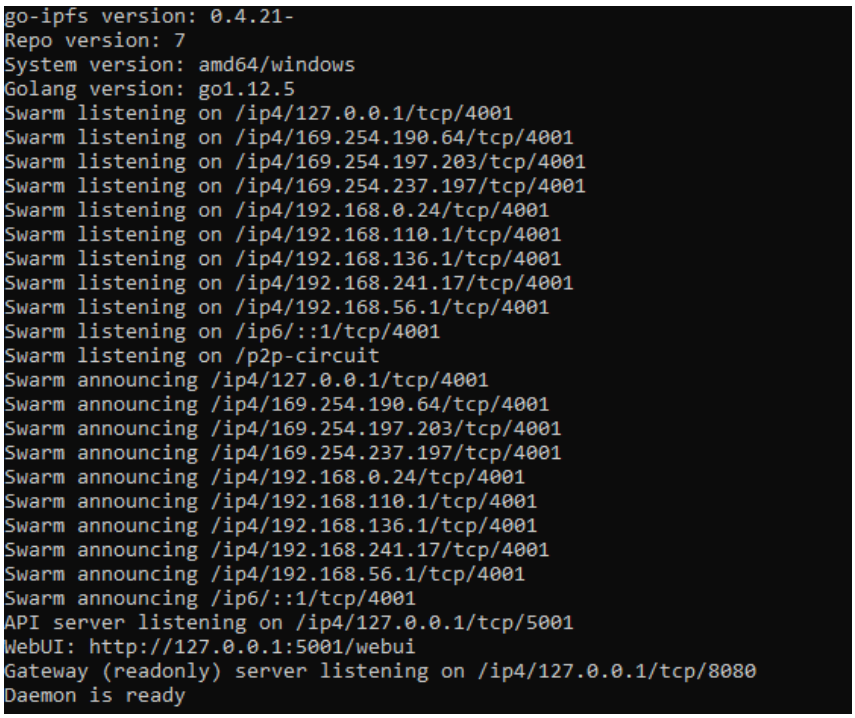
$$\sum\nolimits_1(\mathrm{X}) = ROTR^6(X) \oplus ROTR^{11}(X) ROTR^{25}(X) \tag{3.14}$$

Hàm logic Ch và Maj nhận 3 ký tự làm ngõ vào và trả về 1 ký tự ngõ ra. Kết quả cuối cùng được hình thành bằng công thức:

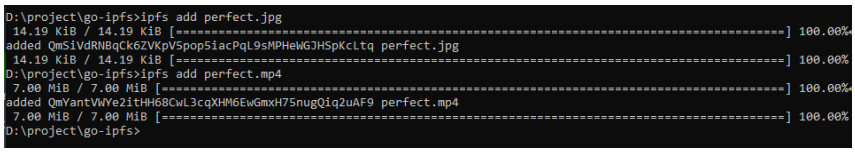
$$SHA256(M) = {H_0}^N \,||\, {H_1}^N \,||\, {H_2}^N \,||\, {H_3}^N \,||\, {H_4}^N \,||\, {H_5}^N \,||\, {H_6}^N \,||\, {H_7}^N \tag{3.15}$$

Để thiết lập địa chỉ cục bộ bằng lệnh `ipfs daemon`. Lệnh này trả về thông tin phiên bản, thông tin và địa chỉ kết nối vào các mạng lưu trữ phân tán (swarm), địa chỉ cho giao diện web.

Nội dung được tải lên bằng lệnh `ipfs add`. Nội dung tệp được tải lên. Kết quả trả về là chuỗi băm đại diện cho nội dung đã được tải lên IPFS.




Hình 3.2: Kết nối nút với các swarm




Hình 3.3: Tải lên nội dung

## 3.2 Mạng blockchain

Nền tảng blockchain có 3 hình thức như đã đề cập, bao gồm: global blockchain, private blockchain, consortium blockchain. Ethereum là nền tảng mạnh mẽ, phổ biến trong global blockchain được đánh giá là một nền tảng phù hợp trong các ứng dụng liên quan đến dịch vụ với quy mô rộng rãi. Trong phạm vi đề tài, Ethereum phù hợp trong ứng dụng mô hình đề xuất thay thế mô hình truyền thống. Đồng thời đóng vai trò là mạng trung tâm của ứng dụng phân phối nội dung video.

Ethereum[16] là một dự án được tạo ra với mục đích đi đầu trong việc sử dụng công nghệ. Là một nền tảng sử dụng công nghệ blockchain, được kết hợp với công nghệ của smart contract (hợp đồng thông minh). Ethereum được tạo ra với mục tiêu trở thành một nền tảng dành cho việc phát triển smart contract và các DApps (nội dung sẽ được đề cập đến ở phần sau của chương). Không giống như Bitcoin[17] được tạo ra nhằm mục đích là trở thành phương tiện thanh toán và nơi lưu trữ giá trị. Cần phân biệt rõ ràng giữa hai nền tảng Bitcoin và Ethereum. Cả hai nền

tảng chạy trên hình thức public blockchain. Điểm khác biệt giữa Bitcoin và Ethereum là tốc độ tạo ra block mới thông qua giao thức GHOST[18] dùng trong Ethereum, bằng cách giảm thời gian xác thực đồng thời lựa chọn nhánh có nhiều nhánh con làm chuỗi chính (mainchain).

Tiền mã hóa (cryptocurrency) là khái niệm tồn tại trong các nền tảng khác nhau, bao gồm: coin và token. Coin là một dạng tiền kỹ thuật số được tạo ra bằng kỹ thuật mã hóa, lưu trữ giá trị theo thời gian. Coin có thể gửi, nhận và đào. Coin không có chức năng nào khác ngoài chức năng tiền tệ. Token được phát hành dựa trên một nền tảng của coin, là một đại diện của một tài sản hoặc tiện ích cụ thể, thường nằm trên một blockchain đã có sẵn. Mã token có tính đa năng hơn khi nó có thể đại diện cho giá trị hàng hóa, thể hiện sự duy nhất của một đối tượng, tích điểm của thành viên, có thể được sử dụng như các loại tiền điện tử để lưu thông.

Token mới được tạo ra trên Ethereum dựa theo chuẩn ERC-20[19]. Chuẩn này định nghĩa một danh sách chung các quy tắc cho Ethereum, các quy tắc gồm các mã thông báo được chuyển giữa các địa chỉ và cách truy cập dữ liệu trong mỗi mà thông báo.

Như đã được đề cập trước đó, Ethereum được tạo ra dùng trong các ứng dụng liên quan đến blockchain cùng với đó là Smart contract tập hợp một bộ giao thức đặc biệt có khả năng tự động thực hiện các điều khoản, các thoả thuận giữa các bên tham gia trong hợp đồng.

Solidity[20] là một ngôn ngữ hướng đối tượng bậc cao được tạo ra nhằm mục đích xây dựng bản hợp đồng thông minh (smart contract) để chạy trên EVM (máy ảo Ethereum). Remix là IDE hay một công cụ giúp việc xây dựng hợp đồng thông minh (smart contract) viết ngay trên trình duyệt, các công cụ khác hỗ trợ việc kiểm thử chương trình, sửa lỗi và biên dịch cũng được hỗ trợ. Thành phần cơ bản của một chương trình gồm: phiên bản của solidity để đảm bảo rằng phiên bản này tương thích với phiên bản biên dịch, các phương thức (hàm) chức năng thực hiện các lệnh, điều khoản trong hợp đồng. Cấu trúc bản hợp đồng (smart contract) có dạng: `pragma solidity ^0.5.1;`

```
contract HelloSolidity {
  function set() {
  }
  function get() {
  }
}
```

Cơ chế các hàm chức năng trong bảng hợp đồng của ứng dụng bao gồm:

- Bổ sung nội dung với các thông đi kèm
- Chức năng bầu chọn cho nội dung

- Trả lợi nhuận cho chủ sở hữu nội dung sau khi được bầu chọn
- Quản lý nội dung, cơ chế bầu chọn nội dung

Quá trình tham gia vào blockchain bắt đầu với một tài khoản đăng nhập, tài khoản này đóng vai trò là người sở hữu nội dung đồng thời chi trả cho việc triển khai nội dung này. Đồng thời cần phải tạo một ví để quản lý tài khoản cũng như là số dư của người dùng, ngoài ra còn có thể đảm bảo được sự an toàn về tài sản của người dùng. Có nhiều ví online đảm bảo độ an toàn về bảo mật và sự tiện dụng trong các giao dịch. Metamask là ví được tin cậy với khả năng bảo mật với một mã nhận diện mã hóa vô cùng an toàn cũng như hỗ trợ nhiều tính năng, tích hợp tốt trong việc phát triển các ứng dụng.

Có 2 loại tài khoản trong blockchain:

- Tài khoản đến từ bên ngoài (Externally own account): tài khoản gồm có cặp khóa, được tạo bởi người dùng hoặc từ các server bên ngoài. Đặc điểm: chứa số dư, có thể khởi tạo giao dịch, không thể triển khai hợp đồng.
- Tài khoản hợp đồng (Contract account): Tài khoản không được kiểm soát bởi con người, có thể kích hoạt từ tài khoản bên ngoài hoặc là tài khoản hợp đồng khác. Đặc điểm: chứa số dư, chứa smart contract trong bộ nhớ, có thể tiến hành kích hoạt các giao dịch hay gọi các hợp đồng khác.

Mỗi hợp đồng được triển khai sẽ phải tiêu tốn một lượng phí để triển khai, phí này được gọi là “Gas”

Khi người dùng gửi một giao dịch (transaction) máy ảo Ethereum yêu cầu một khoản phí nhỏ để thực thi nội dung. Điều này cũng tương tự khi triển khai với smart contract, người dùng phải trả phí cho tiến trình tính toán của hệ thống. Chi phí này được đo bằng đơn vị là “Gas”[17]. Và được trả bằng ether (đơn vị tiền tệ trong Ethereum). Số lượng gas đại diện cho số lượng các chỉ thị phải thực hiện trong một giao dịch, trường hợp trong một hợp đồng phức tạp, yêu cầu nhiều chỉ thị để thực thi hơn đồng nghĩa với mức giá Gas cao hơn. Giao dịch còn yêu cầu giá trị giới hạn Gas (gas limmit), giá trị này cho biết chi phí họ sẵn sàng trả là bao nhiêu cho việc thực thi giao dịch. Tất cả các nút trong mạng đều tham gia mining hay bảo mật mạng cho việc chi trả, cung cấp phần cứng cho việc sao lưu, xác thực. Tiền phí này được các miner nhận như một phần thưởng. Nếu số các bước thực thi giao dịch lớn hơn giá trị giới hạn thì tất cả các bước sẽ trở lại thời điểm ban đầu, không có thành phần nào của giao dịch được thực thi.

Các tiến trình được quy định theo cụ thể theo từng tiến trình:

Bảng 3.1: Giá gas của các tiến trình[17]

| **Tên tiến trình** | **Giá Gas** | **Mô tả** |
|---|---|---|
| step | 1 | Mặc định mỗi bước thực thi |
| stop | 0 | Miễn phí |
| suicide | 0 | Miễn phí |
| sha3 | 20 | Hàm băm SHA-3 |
| sload | 20 | Lấy dữ liệu từ ô nhớ |
| sstore | 100 | Ghi dữ liệu vào ô nhớ |
| balance | 20 | Kiểm tra số dư |
| create | 100 | Khởi tạo hợp đồng |
| call | 20 | Khởi tạo hàm trích xuất |
| memory | 1 | Mỗi từ ghi vào trong bộ nhớ |
| txdata | 5 | Data, code trong giao dịch |
| transaction | 500 | Giao dịch cơ bản |

Không như trong Bitcoin, chi phí cho các giao dịch phụ thuộc vào kích cỡ của các transaction theo đơn vị kilobytes. Trong trong solidity thì dựa trên số lượng công việc phải giải quyết trong một giao dịch cụ thể.

Trong nội dung nghiên cứu, sử dụng global public blockchain cùng với Metamask có hỗ trợ Web3. Web3 là trung gian kết nối với mạng blockchain trong triển khai hợp đồng. Sau khi môi trường thích hợp được chọn, người dùng sẽ xác nhận một lần nữa tài khoản được chon để triển khai hợp đồng. Thông qua Remix, hợp đồng sẽ được biên dịch ra bytecode.

Web3[21] là bộ các thư viện cho phép truy nhập vào mạng local hay nút ethereum từ xa thông qua kết nối HTTP và IPC. Web3 là công cụ hỗ trợ trong tiến trình kết nối, trao đổi dữ liệu hay tương tác với mạng blockchain.

Việc triển khai hợp đồng là một tiến trình đầu tiên khi đưa nội dung lên mạng blockchain. Bao gồm:

- Đưa mã băm (hash) của nội dung vào hợp đồng thông minh: mã băm sau khi đưa nội dung lên IPFS sẽ được đưa vào trong smart contract.
- Lựa chọn môi trường, tài khoản, các thông số để triển khai hợp đồng: sử dụng môi trường cup cấp của Web3, chọn tài khoản từ ví Metamask. Lựa chọn giá trị của gas limit.

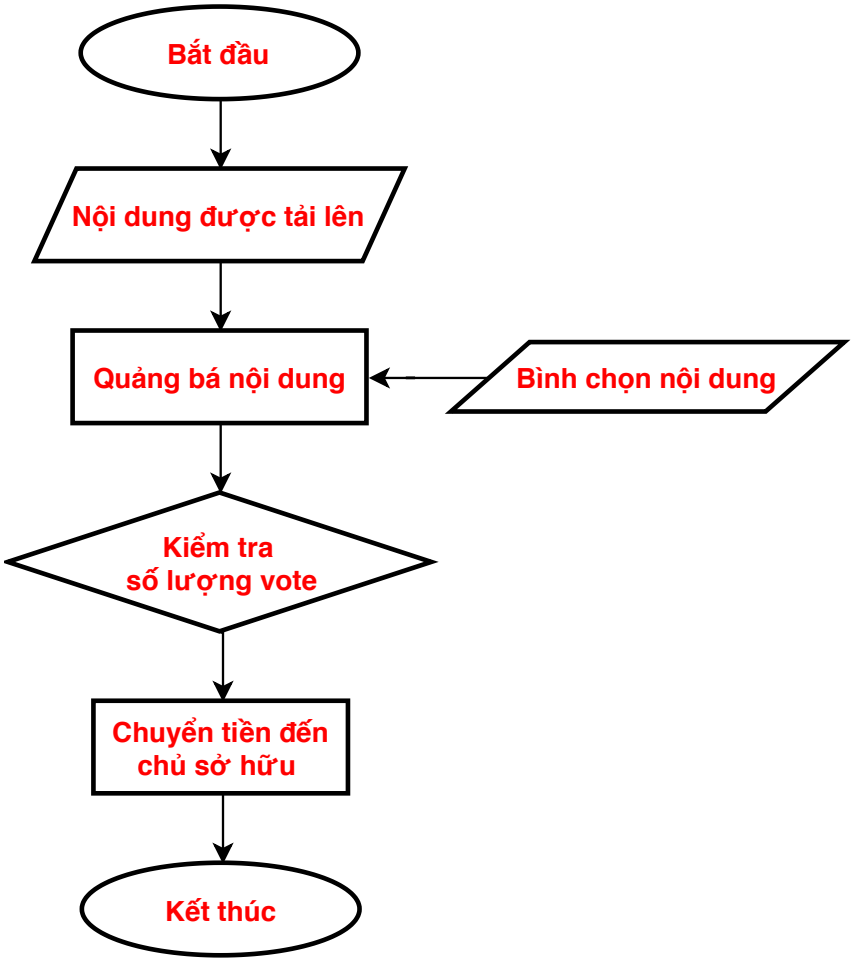
Hợp đồng sau khi được triển khai, có thể xem là một giao dịch hay một transaction diễn ra, tại cửa sổ terminal được tích hợp bộ phiên dịch Javascript, chỉ contract trả về trên cửa sổ này đồng nghĩa với việc triển khai nội dung thành công. Địa chỉ hợp đồng là kiểu dữ liệu địa chỉ dưới dạng Hexa gồm 20 bytes[20]. Mô hình đề xuất trong nghiên cứu sử dụng mạng thử nghiệm Rospten được tạo ra nhằm mục đích phát triển với tính năng tương tự như mạng thật cho nhà phát triển tương tác trước khi sử dụng mạng thật.

## 3.3 Khối tương tác người dùng

Việc truy xuất vào hợp đồng đứng từ vị trí của một người dùng tham gia vào mạng blockchain cần 2 thông số: địa chỉ hợp đồng, ABI (Application Binary Interface) của hợp đồng. Thông qua Etherscan là một công cụ blockchain explorer được tạo ra để sử dụng riêng đối với nền tảng Ethereum, thông qua đó có thể kiểm tra các giao dịch ETH trên nền tảng, các thông tin về các block, smart contract cũng như theo dõi được các giao dịch ở các nền tảng phi tập trung dựa trên blockchain của Ethereum. Có thể xem rằng Etherscan như là một giao diện cho sổ cái, khi các thông số liên quan đến tài khoản về số dư, quản lý nội dung hợp đồng hay các giao dịch diễn ra được người dùng theo dõi.

Thông thường, người dùng muốn tham gia vào mạng blockchain nói chung hay Ethereum nói riêng cần phải cải đặt về thông tin sổ cái hay phải chạy toàn bộ nút trong mạng. Infura là công cụ phía back-end hỗ trợ trong việc giả lập một nút từ xa nhằm đơn giản hóa các nền tảng yêu cầu của một mạng blockchain. Với mục đích hỗ trợ các ứng dụng sử dụng nền tảng blockchain, Infura là công cụ giải quyết nhanh các vấn đề về nền tảng.

Xây dựng nền ứng dụng tương tác người dùng thông qua Reactjs trên nền tảng Nodejs nhằm tăng tốc độ ứng dụng. Thông qua thư viện Web3, người dùng sẽ tham gia vào mạng blockchain để tương tác với hợp đồng (smart contract), tiến hành các yêu cầu trao đổi dữ liệu và nội dung.




Hình 3.4: Lưu đồ hoạt động trong ứng dụng

Người dùng sử dụng nền tảng để tải lên nội dung, nội dung này gắn liền với một tài khoản ví. Sau khi được đưa lên IPFS và xác thực vào mạng blockchain thông qua smart contract, nội dung lúc này sẽ công khai đến các người dùng khác. Người dùng sẽ xem nội dung và bình chọn cho nội dung. Lúc nội dung được số lượng bình chọn nhất định, chủ sở hữu nội dung sẽ nhận được phần thưởng từ nền tảng. Ứng dụng người dùng lúc này gọi là DApp (decentralized application).

# CHƯƠNG 4

# ĐÁNH GIÁ MÔ HÌNH ĐỀ XUẤT, PHƯƠNG HƯỚNG PHÁT TRIỂN

## 4.1 IPFS server

Do IPFS không phải là một mô hình mạnh mẽ dành cho kinh doanh. Mô hình này không thể tự nó mở rộng dung lượng lưu trữ như là một dịch vụ lưu trữ đúng nghĩa. IPFS phải phụ thuộc vào các nút tham gia với mục đích duy trì khả năng lưu trữ theo đúng cơ chế. Quay trở lại mô hình phân phối đề xuất, IPFS ở vị trí đầu chuỗi tiến trình, chịu trách nhiệm tiền xử lý, là nơi lưu trữ nội dung biến đổi dạng nội dung thành một chuỗi băm thông qua hàm băm (hash function). Kích thước nội dung sẽ không ảnh hưởng trực tiếp đến ứng dụng, tuy nhiên thời gian tải lên IPFS server và tiến trình lấy nội dung sẽ không diễn ra một cách hoàn hảo. Trường hợp số nút trên IPFS server quá ít, trong khi nội dung đưa lên quá nhiều, không gian lưu trữ trên IPFS sẽ không đáp ứng được, mô hình không thể hoạt động. Hướng giải quyết vấn đề vẫn còn hạn chế phụ thuộc vào độ quy mô của IPFS.

Một vấn đề khác cần quan tâm là cơ chế sao lưu dữ liệu trong mạng ngang hàng. Với mục đích hạn chế tình trạng mất dữ liệu do các nút tham gia lưu trữ dữ liệu không đi vắng (không tham gia vào mạng ở một thời điểm nhất định) đảm bảo nội dung luôn tồn tại trên mạng, mặt khác nhằm tránh vấn đề có quá nhiều yêu cầu dữ liệu từ nhiều nút khác đến cùng lúc. Thuật toán cho cơ chế sao lưu điều chỉnh các nút chứa dữ liệu được sao lưu dựa trên lưu lượng trong các phương thức phân tán trong việc giải quyết việc tăng số lượng dữ liệu yêu cầu[22]. Tỉ lệ truy vấn của dữ liệu được biểu diễn bằng thông số $q_f$ được xem là giá trị truy vấn ban đầu trong khoảng thời gian $T$. Hiệu năng sao lưu dữ liệu được đặt là một giá trị ngưỡng cho tỉ lệ truy vấn, $T_q = \alpha * avg_q$ với $\alpha$ ($\alpha \geq 2$) là hằng số, $avg_q$ là tỉ lệ truy vấn trung bình trong mạng, $n_f$ là giá trị số lượng tệp dữ liệu trong mạng. Giá trị tỉ lệ truy vấn trung bình được xác định bởi công thức:

$$avg_q = \sum_{j=1}^{n_f} \frac{q_{f_j}}{n_f} \tag{4.1}$$

Bảng 4.1: Giá trị sao lưu với số lượng truy xuất thay đổi trong khoảng thời gian $T = 1s$, số lượng dữ liệu trong mạng $q_f = 4$ và hằng số $\alpha = 2$

| **Số lượng truy vấn** | **Giá trị truy vấn trung bình** | **Hiệu quả sao lưu** |
|---|---|---|
| 1 | 1 | 2 |
| 2 | 2 | 4 |
| 3 | 3 | 6 |
| 4 | 4 | 8 |
| ... | ... | ... |
| n | n | 2n |

Với số lượng truy vấn như nhau ở các phiên dữ liệu được yêu cầu, tỉ lệ thuận với giá trị truy vấn trung bình $avg_q$ cũng như hiệu quả cơ chế sao lưu này. Với nhiều yêu cầu truy vấn, hệ thống cần nhiều dữ liệu được sao lưu hơn trong hệ thống.

Không mã hóa dữ liệu, thiếu cơ chế bảo mật dữ liệu hiệu quả, khiến cho việc lưu trữ hay truyền dữ liệu trở nên kém hiệu quả. Không có cơ chế bảo vệ độ tin cậy dữ liệu khi cập nhật lên phiên bản mới nhất là những hạn chế phải đánh đổi, nền tảng chỉ thích hợp với yêu cầu tăng tốc phản hồi các yêu cầu, không thích hợp với thị trường lưu trữ lâu dài và lưu trữ dữ liệu người dùng cá nhân hay doanh nghiệp. Không khó để nhận ra nền tảng được sử dụng chỉ là hệ thống phân phối không phải là một trung tâm dữ liệu thuần.

IPFS và blockchain là hai thành phần phù hợp với nhau do những sự tiện lợi, hay các tính năng sự tương đồng về cách thức hoạt động và vận hành. IPFS hỗ trợ blockchain rất nhiều tiêu biểu nhất là nội dung với kích thước bất kì được biến thành một chuỗi và đưa vào trong blockchain thông qua hợp đồng (smart contract). Giải quyết vấn đề lưu trữ trong blockchain do không gian lưu trữ dành cho dữ liệu không được nhiều.

IPFS không tối ưu trong việc riêng tư hóa dữ liệu, kết quả là không hiệu quả khi đưa dữ liệu mã hóa vào bộ nhớ cache, khi mà chỉ người sở hữu mới biết được những nội dung này.

Trong tiến trình tải lên nội dung, có nhiều nội dung với các kích thước khác nhau. Yêu cầu về kích thước giới hạn cho các tệp tải lên là không giới hạn. Tuy nhiên, vẫn có thể tùy chọn kích thước tải xuống tùy theo yêu cầu.

Các nội dung có dung lượng lớn cần một khoảng thời gian lớn hơn để video được tải lên, cũng tương tự như nội dung có dung lượng thấp hơn thì cần ít hơn thời gian thực hiện. Các nút tham gia trong quá trình tải lên cũng ảnh hưởng tùy vào dung lượng của nội dung tải lên. Theo

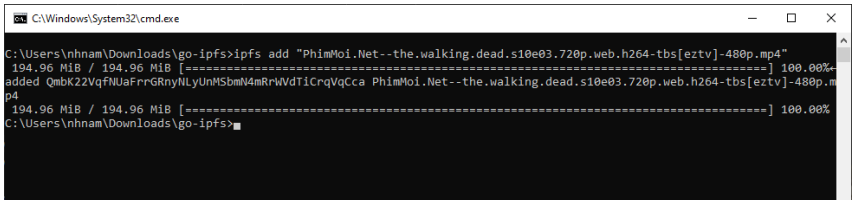
cơ chế, nội dung được tải lên phân chia thành các gói và lưu trữ tại các nút. Tuy nhiên, các nút mang dữ liệu rời khỏi mạng khi không hoạt động dữ liệu lúc này sẽ mất đi. Do đó cần phải có cơ chế đảm bảo IPFS duy trì dữ liệu cần thiết. Dữ liệu chứa trong một liên kết không vượt quá 256 KB, trường hợp dữ liệu vượt hơn 256KB, nó sẽ được chia thành nhiều phần có kích thước nhỏ hơn 256 KB.

Bảng 4.2: Các thông số quá trình tải lên nội dung trong trong IPFS

| Kích thước | Liên kết | Block Size | Data Size | Link Size | Tổng |
|---|---|---|---|---|---|
| **3. 94 MiB** | 16 | 777 | 71 | 706 | 4134430 |
| **6. 09 MiB** | 25 | 1209 | 107 | 1102 | 6389296 |
| **7. 0 MiB** | 29 | 1399 | 122 | 1277 | 7344402 |
| **24. 64 MiB** | 99 | 4762 | 403 | 4359 | 25847769 |
| **34. 93 MiB** | 140 | 6730 | 567 | 6163 | 36623518 |

Nội dung tải lên có kích thước càng lớn cần nhiều liên kết hay cần nhiều khối để lưu trữ dữ liệu dựa trên nguyên lý lưu trữ của IPFS. Các đơn vị lưu trữ trong từng khối được phân biệt thành: kích thước dữ liệu thực tế cùng với đó là kích thước liên kết. Kích thước liên kết này chứa thông tin địa chỉ đến khối tiếp theo. Theo đó, mỗi liên kết là một địa chỉ chứa trong DAG.

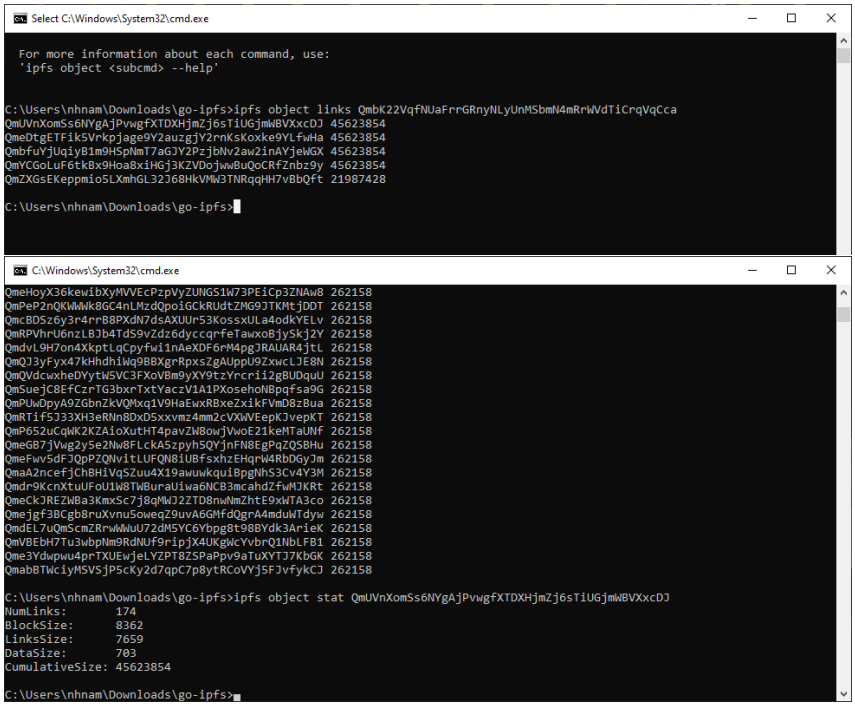
Trường hợp nội dung được tải lên IPFS có kích thước quá lớn vượt quá kích thước cho phép, hệ thống sẽ nhóm mỗi 174 liên kết vào một nhóm. Lúc này hệ thống sẽ tổ chức thành các nhóm phân cấp, chứa lần lượt đến hết số lượng dữ liệu đã phân mảnh.



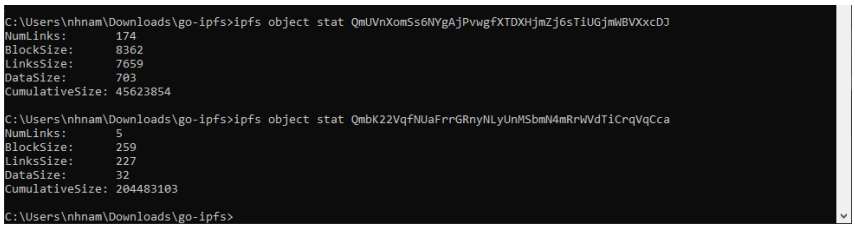

Hình 4.1: Nội dung tải lên với kích thước lớn

Ví dụ minh họa cho nội dung tải lên có kích thước 194.96 MiB

Với tệp tải có kích thước lớn, hệ thống nhóm mỗi 174 liên kết thành một liên kết lớn vẫn đảm bảo mở trong mỗi object không vượt quá kích thước quy định. Từ đó, có thể thấy được rằng, qui định kích thước tối đa trong một liên kết là 262158 đơn vị byte, kích thước tối đa trong một liên kết lớn là 45623854 bytes.




Hình 4.2: Nhóm các object trong lưu trữ nội dung tải lên




Hình 4.3: Các liên kết trong lưu trữ nội dung

Bảng 4.3: Các thông số quá trình tải lên nội dung với kích thước lớn

| Kích thước | Liên kết | Block Size | Data Size | Link Size | Tổng |
|---|---|---|---|---|---|
| **194. 96 MiB** | 5 | 259 | 32 | 227 | 204483103 |
| * | 174 | 8362 | 703 | 7659 | 45623854 |

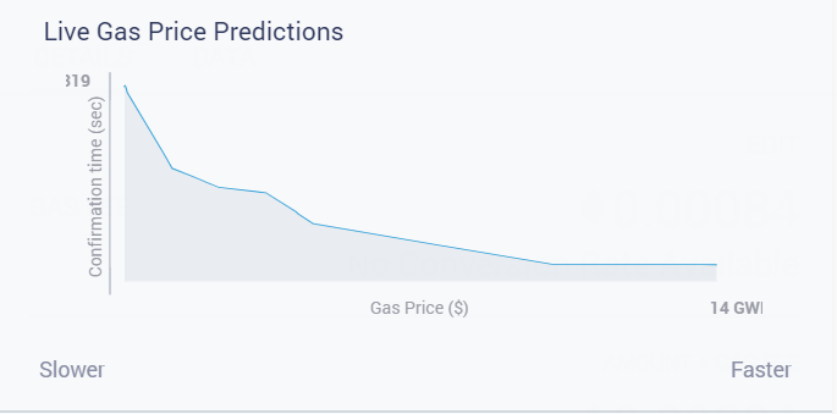
Mặt khác việc không thể chủ động điều chỉnh số lượng các khối trong quá trình phân mảnh nội dung được tải lên đồng nghĩa với việc thay đổi thời gian tải lên hay tải xuống trong trường hợp không sử dụng mạng để mô phỏng đánh giá hệ thống một cách tường minh.

## 4.2 Mạng Blockchain

Với đặc tính tương tự IPFS, nền tảng Ethereum sử dụng trong xây dựng mô hình đề xuất hạn chế rất nhiều trong thời gian xác thực. Xét trong mạng Rospten thuộc nền tảng Ethereum, khi xây dựng một hợp đồng tương đương thì thời gian để xác thực là rất lớn. Tuy nhiên, theo cơ chế được đặt ra nhằm cải thiện thời gian xác thực cho các hợp đồng, giá trị của hợp đồng tăng lên đồng nghĩa hợp đồng này sẽ được đưa lên đầu của hàng đợi tăng mức độ ưu tiên đối với hợp đồng này.


Hình 4.4: Tùy chỉnh giá trị gas

Giải pháp tăng tốc độ xử lý này gây ra nhiều lãng phí trong các ứng dụng, giá gas có thể tăng lên theo đơn vị GWEI mà không vượt quá hạn mức gas (Gas Limit) đồng thời không vượt quá số dư trong ví (theo đơn vị ETH). Theo đó, giá trị tổng lúc này để xác thực hợp đồng sẽ tăng lên, thời gian ước tính cho quá trình xác thực sẽ giảm xuống. Mối quan hệ giữa giá gas và thời gian xác thực được thể hiện với biểu đồ:




Hình 4.5: Dự đoán giá trị gas và thời gian xác thực hợp đồng

Trong mỗi hợp đồng được xác thực, tập tin lưu trữ giao dịch (transaction) ghi nhận các thông

tin liên quan đến thời gian với giá trị timestamp, đây là giá trị ghi nhận thời gian theo hệ thống Unix, mang thông tin về ngày, giờ , phút, giây theo UTC (mốc thời gian ban đầu lúc 00:00:00 ngày 01/01/1970) khi một khối được hình thành.

Các hợp đồng (Smart contract) khác nhau về dung lượng và số gas theo đó thời gian xác thực cũng khác nhau. Đối với các ứng dụng có hợp đồng phức tạp, yêu cầu số lượng gas lớn để xác thực trên mạng blockchain, sẽ gây trở ngại cho những nhà đóng góp nội dung mặc dù phần thưởng nhận được từ những nội dung của họ lớn hơn rất nhiều chi phí bỏ ra cho việc xác thực giao dịch nói chung và các tính năng tương tác với mạng blockchain nói riêng.

Mô hình ứng dụng đề xuất gồm có 3 tính năng tương tác chính:

- Tải lên nội dung: Người dùng sẽ tải lên nội dung với một tài khoản tồn tại số dư. Với chi phí được tính cho từng nội dung tải lên. Nội dung được tải lên sẽ gắn với nội dung của tài khoản người dùng. Người dùng này sẽ chịu trách nhiệm cho nội dung của mình kể cả khi nhận phần thưởng hay chịu phạt từ ứng dụng.

- Tính năng chia sẻ nội dung: Nội dung được bất kì người dùng nào tải lên đều được quảng bá trên mục tùy chọn video của ứng dụng. Người dùng khác có thể tùy chọn nội dung để xem tại đây mà không mất phí.

- Bình chọn nội dung: Mỗi nội đung trong mục tùy chọn khi được quảng bá đều kèm với chức năng bình chọn nội dung. Với chức năng này, người bình chọn sẽ mất phí cho mỗi lượt bình chọn, phía ngược lại, chủ sở hữu nội dung sẽ nhận được phần thưởng từ ứng dụng với số lượt bình chọn đạt mức theo quy định.

Mô hình đề xuất đã giải quyết được cơ bản các vấn đề hiện tại đang tồn tại trong mô hình truyền thống thông qua bảng so sánh.

Bảng 4.4: Đặc tính đóng góp của mô hình đề xuất

| **Mô hình tập trung** | **Mô hình đề xuất** |
|---|---|
| Tiền xử lý nội dung | **Tải lên trực tiếp nội dung** |
| Lưu trữ ở trung tâm dữ liệu (database) | **Lưu trữ ở mạng phi tập trung IPFS** |
| Server quản lý, phân phối nội dung | **Smart contract định tuyến, phân phối nội dung** |
| Server quyết định, điều khiển các tiến trình | **Blockchain là nơi chứa Smart contract** |
| Số lượng truy cập giới hạn ở băng thông | **Không hạn chế số lượng truy cập** |
| Giao dịch, chức năng không tường minh | **Phương thức nhận thưởng** |

Do nội dung sẽ được xử lý trên mạng IPFS do đó nội dung không cần phải trải qua bước tiền xử lý trước ở ngõ vào IPFS server. Cùng với đó, các thông tin, cơ chế vận hành ứng dụng được thiết lập trong Smart contract, các thực thể tham gia vào ứng dụng dựa vào các nguyên tắc được định sẵn trong Smart contract này để hoạt động. Đối với mô hình đề xuất, phương thức nhận thưởng sẽ tùy vào từng bình chọn của người dùng đối với nội dung, cùng với số lượng đạt ngưỡng để nhận thưởng. Ở các ứng dụng tương tự, từng bình chọn sẽ mang một giá trị nhận thưởng giá trị này có thể điều chỉnh thông qua chủ sở hữu nội dung trong giai đoạn tải lên.

Các tính năng tích hợp trên ứng dụng cơ bản giải quyết được các chức năng cơ bản theo yêu cầu của một nền tảng cung cấp nội dung video. Tuy thế, những hạn chế vẫn còn ở các tính năng này. Mang tính chất của một framework do đó hạn chế ở các tính năng là điều khó tránh khỏi.

- Tải lên nội dung: Nội dung được tải lên IPFS server với thời gian lớn (25 giây) cho mỗi nội dung video có kích thước từ 4 đến 7 MB. Không có thể hiện được tiến tình tải lên.
- Tính năng chia sẻ nội dung: Trang cần được làm mới để cập nhật nội dung trong lúc nội dung được người dùng khác tải lên liên tục.
- Bình chọn nội dung: Người quản lý nội dung có thể bình chọn cho chính nội dung của mình, dựa vào điểm này có thể lấy tiền từ ứng dụng. Chưa có nội dung downvote nhằm báo cáo nội dung không phù hợp. Mặt khác, một người dùng có thể bình chọn nhiều lần cho một nội dung.

So sánh mô hình đề xuất với mô hình đã hoạt động sử dụng công nghệ blockchain DTube[5]

Bảng 4.5: So sánh tính năng của mô hình đề xuất và dịch vụ DTube

| **Tính năng** | **Mô hình đề xuất** | **Dịch vụ DTube** |
|---|---|---|
| Hình thức tải lên nội dung | Tệp nội dung | Tệp + địa chỉ URL |
| Chi phí tải lên | Có tính phí (theo ETH) | Có tính phí (theo DTC) |
| Quản lý người dùng | Thông qua ví Metamask | Mã riêng tư của DTube |
| Bình chọn nội dung | Tốn phí | Không tốn phí |
| Hình thức bình chọn | Đạt mốc nhận thưởng | Phần thưởng cộng dồn cho từng lượt |
| Giới hạn bình chọn | Không giới hạn | Một người dùng/nội dung |

Nhìn chung, các chức năng trong DTube ngoại trừ tải lên nội dung đều không tin phí. Một ưu điểm khác của ứng dụng này còn ở việc bảo quản lý tài khoản với các thông tin ràng buộc

chặt chẽ. Một điểm khác trong dịch vụ DTube công khai số lượng thưởng của một nội dung với mục đích tường minh cơ chế nhận thưởng. Theo lý thuyết, mọi sự quản lý đều được thực hiện một cách hoàn toàn tự động, tuy nhiên trong thực tế chỉ có 90% hệ thống được thực hiện tự động, còn lại được nhà quản lý ứng dụng can thiệp trong các tính năng quản lý tài khoản cũng như tìm kiếm lợi nhuận.

## 4.3 Chi phí xây dựng dịch vụ

Đối với các mô hình phân phối video tập trung sử dụng dịch vụ bên thứ 3 như một thành phần trung gian đảm nhận vai trò lưu trữ, xử lý phân luồng nội dung đến người dùng. Ước tính điển hình khi sử dụng các dịch vụ, cụ thể dịch vụ của Muvi[23] với gói tùy chọn cho nền tảng phân phối video Muvi Professional và Muvi Enterprise với các tính năng:

Bảng 4.6: Các hình thức dịch vụ và các tính năng của Muvi[23]

| **Hình thức** | **Muvi Professional (1499 USD)** | **Muvi Enterprise (3900 USD)** |
|---|---|---|
| Số lượng nội dung | Không giới hạn | Không giới hạn |
| Băng thông/Tháng | Miễn phí 2TB | Miễn phí 5TB |
| Dung lượng | Miễn phí 2TB | Miễn phí 5TB |
| Người dùng đồng thời | 10000 | Không giới hạn |

Trong khi đó, một dịch vụ về hệ thống nội dung khác đó là Wowza[11] cũng có các tùy chọn cho dịch vụ Wowza Streaming Cloud với các tính năng: Chất lượng hình ảnh trên các thiết bị streaming, không giới hạn thiết bị ở các nền tảng khác nhau, khả năng mở rộng server với dung lượng không giới hạn, bảo mật nội dung với các cơ chế tùy chọn, tính năng tùy chọn danh sách nội dung. Đó là các nội dung cơ bản trong các gói dịch vụ được cung cấp với mức giá 2495 USD/tháng.

Trong quá trình vận hành của mô hình đề xuất, yêu cầu một lượng lớn chi phí vận hành phía nhà quản lý cũng như người tham gia ứng dụng.

Các chi phí vận hành cho từng chức năng trong ứng dụng được từ phía người dùng và nhà quản lý với nguyên tắc càng xử lý nhiều yêu cầu trong chức năng thì chi phí bỏ ra để thực hiện chức năng đó trong tương tác với mạng blockchain càng lớn, cụ thể:

| Tiến trình | Chi phí | VND |
|---|---|---|
| Triển khai hợp đồng | 0.00084 ETH | 6,688,649.66 VND |
| Tải lên nội dung 1 | 0.005728 ETH | 19,148.25 VND |
| Tải lên nội dung 2 | 0.004386 ETH | 14,662.05 VND |
| Tải lên nội dung 3 | 0.004391 ETH | 14,678.77 VND |
| Upvote 1 | 0.001303 ETH | 4,355.83 VND |
| Upvote 2 | 0.000853 ETH | 2,851.51 VND |
| Upvote 3 | 0.000853 ETH | 2,851.51 VND |
| Nhận thưởng | 0.000985 ETH | 3,292.78 VND |

Trong phạm vi ứng dụng, xem xét các giải pháp sử dụng các dịch vụ bên thứ ba với tùy chọn tính năng cao nhất cho mô hình phân phối video tập trung, chi phí đầu tư cho một ứng dụng với tầm nhìn lớn tại Việt Nam thì phù hợp với giải pháp Muvi Professional với các tính năng đã đề cập. Tuy nhiên, các ước tính chi phí trên chưa bao gồm các chi phí xung quanh việc mua bán bản quyền nội dung. Với nhìn nhận hiện tại, con số để triển khai sẽ còn tiếp tục tăng.

Trong mô hình đề xuất, với chi phí lớn cho việc vận hành từ nhà quản lý cho ứng dụng, cụ thể là chi phí triển khai hợp đồng, yêu cầu phải được lặp lại theo chu kì trong khi lợi nhuận thu được chỉ nhờ vào việc phát hành token cho hệ thống. Song theo đó, người dùng phải mất tiền cho các thao tác của mình với chức năng trong ứng dụng mô hình sẽ đảm bảo cho vấn đề về bản quyền. Vì được xây dựng trên nền tảng Ethereum, sự phụ thuộc vào giá trị của đồng ETH là việc khó tránh khỏi. Không như mô hình phân phối tập trung, chi phí cho băng thông, số lượng hay kích thước nội dung sẽ được giảm bớt. Chi phí có thể kiểm soát được trong ứng dụng tùy vào các đợt phát hành token cho ứng dụng từ nhà quản lý. Cũng giống như mô hình được triển khai đã phân tích, chi phí bản quyền nội dung chưa được tính đến trong phép ước tính này.

## 4.4 Hướng phát triển

Với các đặc tính của hệ thống phân tán, mô hình đã giải quyết cơ bản về băng thông trong ứng dụng cũng như các vấn đề về quá tải server tập trung. Với sự xuất hiện các nền tảng phù hợp trong công nghệ blockchain, phần nào đó đã đa dạng hóa các tính năng của ứng dụng. Nếu như về các tính năng hỗ trợ trong ứng dụng toàn cầu, Ethereum là một nền tảng lý tưởng song theo đó một số hạn chế về các đặc tính xác thực. Hyperledger xuất hiện để thay đổi các vấn đề này, với những tính năng chặt chẽ trong kết cấu, nền tảng tiêu biểu cho loại Permissioned blockchain. Với tính năng tùy biến để có thể đáp ứng các yêu cầu đặc trưng của ứng dụng, tuy vậy chỉ có thể dừng lại trong ứng dụng có quy mô nhỏ.

Trong phạm vi mạng blockchain riêng biệt, việc thay thế cơ chế xác thực PoW (Proof of Work) cùng sự hiểu quả đến từ việc xác thực, tuy nhiên rất tốn kém trong yêu cầu năng lượng tiêu thụ đối với cơ chế này, cơ chế PoS (Proof of Stake) trở thành đối tượng được chọn với việc đảm bảo sự đồng thuận mà không cần mining sẽ giảm được năng lượng hao phí cũng như sự cần thiết đảm bảo cho mục đích chống lạm phát. Hơn nữa, khối được xác thực sẽ nhanh hơn đảm bảo cho cơ chế bảo mật chặt chẽ hơn.

Với khả năng mở rộng các tính năng quan trọng, bảo mật nội dung là điều cần thiết. Do không có cơ chế bảo mật chủ động ở dịch vụ IPFS nên việc bảo mật nội dung từ khối IPFS trong mô hình xây dựng là điểm quan trọng trong tiến trình vận hành ứng dụng. Mã hóa bất đối xứng (Asymmetric Encryption) là một công cụ cho phép mã hóa nội dung bằng khóa công khai định cho người nhận và chỉ có người nhận mới có thể giải mã sau khi yêu cầu dữ liệu từ IPFS. Các yếu tố khác không thể tấn công và đồng thời không thể giải mã được, bất chấp việc có thể lấy thành công dữ liệu từ IPFS.

Trong phạm vi đề tài chỉ dừng lại ở bước xây dựng framework cho ứng dụng phân phối video nên các tính năng trong ứng dụng còn hạn chế. Chức năng tìm kiếm nội dung sẽ được phát triển với sự tăng lên về người tham gia cũng như lượng lớn nội dung. Dễ dàng quản lý nội dung hơn với chức năng tìm kiếm hay phân biệt theo các loại nhãn. Sử dụng Machine learning trong tính năng gợi ý nội dung dựa trên các nhãn đã phân loại trước đó, những nội dung có liên quan nội dung người dùng xem nhiều sẽ được ưu tiên xuất hiện với tần xuất nhiều hơn. Quản lý người dùng cũng là một vấn đề cần thiết trong khi mô hình hiện tại việc phân biệt người dùng lại thông qua địa chỉ ví hạn chế trong việc nhận dạng hay phân biệt.

Doanh nghiệp có thể tham gia vào ứng dụng để quảng cáo sản phẩm của riêng mình, người dùng có thể nhận được phần thưởng thông qua xem những quảng cáo này. Ở tính năng này, ngoài chi phí được phải chi cho việc xác thực hợp đồng, phía nhà quảng cáo cũng cần phải mất thêm một khoảng thưởng cho người xem quảng cáo. Lúc này, ứng dụng sẽ gồm ba nhóm đối tượng: người dùng, người đóng góp nội dung và nhà quảng cáo, trong đó người dùng và người đóng góp nội dung có thể là một. Với các tính năng được cải thiện cũng như bổ sung trong định hướng phát triển, các ứng dụng với công nghệ blockchain hứa hẹn sẽ thay thế dần các mô hình truyền thống trong tương lai không xa.

# KẾT LUẬN

Blockchain là công nghệ đầy hứa hẹn với những tính năng mạnh mẽ trong tương lai với sức mạnh nổi bật trong bảo mật thông được củng cố bởi các cơ chế đồng thuận, những thành phần hỗ trợ nhau trong hệ sinh thái mang đến khả năng thích hợp trong các ứng dụng hay các nền tảng được phát triển sau này.

Đề tài với mục đích tạo ra một framework khắc họa tổng quan ứng dụng nền tảng video, giải quyết cơ bản các vấn đề về sử dụng cơ chế quản lý tập trung cũng như lưu trữ dữ liệu theo cách truyền thống. Mạng blockchain, nền tảng Ethereum được dùng trong phân phối nội dung, ứng dụng giờ đây không còn sử dụng server trung tâm, giải quyết vấn đề băng thông, hay lưu lượng các yêu cầu từ phía người dùng trở, tình trạng quá tải ở server như trong các ứng dụng trước đó. Với IPFS thay thế trung tâm dữ liệu (Data center) trong lưu trữ nội dung của ứng dụng, IPFS sử dụng mạng phân tán trong lưu trữ đảm bảo được nguyên vẹn nội dung, với cơ chế sao lưu, nội dung được lưu trữ khó bị mất đi. Với việc phân chia người dùng thông qua sử dụng tài khoản ví Metamask, ứng dụng mang đến một kiểu tên người dùng mới thông qua địa chỉ ví vừa đại điện vừa là công cụ thanh toán cho các giao dịch thực hiện trong nền tảng.

Với những vấn đề chính phần nào được giải quyết trong đề tài, tuy nhiên vẫn còn đó những hạn chế chưa thể khắc phục cho công nghệ mới, về sự hạn chế của nền tảng Ethereum trong quá trình xác thực các giao dịch hay các bản hợp đồng. Yêu cầu cơ bản của đa số các ứng dụng liên quan đến thời gian phản hồi, bên cạnh những bước xác thực không cần thiết, theo đó là các khoản phí cho những cơ chế tương tác với mạng blockchain. Đòi hỏi rất nhiều tài nguyên để vận hành các ứng dụng trong thực tế.

# TÀI LIỆU THAM KHẢO


[1] Z. Zheng et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. June 2017, pp. 557–564. DOI: 10.1109/BigDataCongress.2017.85.

[2] Satoshi Nakamoto et al. “Bitcoin: A peer-to-peer electronic cash system”. In: (2008).

[3] Julija Golosova and Andrejs Romanovs. “The Advantages and Disadvantages of the Blockchain Technology”. In: Nov. 2018, pp. 1–6. DOI: 10.1109/AIEEE.2018.8592253.

[4] Sarah Perez. *"Spotify acquires blockchain startup Mediachain to solve music's attribution problem"*. 2017. URL: https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediachain-to-solve-musics-attribution-problem/ (visited on 09/21/2019).

[5] Elie Majorel Jérémy Lair André. *Turning the tables in the social media industry*. Tech. rep. June 2019. URL: https://d.tube/.

[6] Stan Abraham. “Will business model innovation replace strategic analysis?” In: *Strategy & Leadership* 41.2 (2013), pp. 31–38.

[7] Lothar Mikos. “Digital Media Platforms and the Use of TV Content: Binge Watching and Video-on-Demand in Germany”. In: *Media and Communication* 4.3 (2016), pp. 154–161. ISSN: 2183-2439. DOI: 10.17645/mac.v4i3.542. URL: https://www.cogitatiopress.com/mediaandcommunication/article/view/542.

[8] Danielle M Soulliere. “Wrestling with masculinity: Messages about manhood in the WWE”. In: *Sex Roles* 55.1-2 (2006), pp. 1–11.

[9] Paul Covington, Jay Adams, and Emre Sargin. “Deep neural networks for youtube recommendations”. In: *Proceedings of the 10th ACM conference on recommender systems*. ACM. 2016, pp. 191–198.

[10] Adobe Sys. *Inc. v. Wowza Media Sys. Inc., No*. Tech. rep. CV-11-02243,(ND Cal. filed May 6, 2011), Declaration of Milan Toth, 2011.

[11] LLC. Wowza® Media Systems. *Wowza Streaming EngineTM – Overview*. Tech. rep. February 2014.

[12] Nishara Nizamuddin, Haya R Hasan, and Khaled Salah. “IPFS-blockchain-based authenticity of online publications”. In: *International Conference on Blockchain*. Springer. 2018, pp. 199–212.

[13] Juan Benet. “Ipfs-content addressed, versioned, p2p file system”. In: *arXiv preprint arXiv:1407.3561* (2014).

[14] Scott Chacon and Ben Straub. *Pro git*. Apress, 2014.

[15] Rahul P Naik and Nicolas T Courtois. “Optimising the SHA256 Hashing Algorithm for Faster and More Efficient Bitcoin Mining”. In: *MSc Information Security Department of Computer Science UCL* (2013), pp. 1–65.

[16] Gavin Wood et al. “Ethereum: A secure decentralised generalised transaction ledger”. In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.

[17] Chris Dannen. *Introducing Ethereum and Solidity*. Springer, 2017.

[18] Yonatan Sompolinsky and Aviv Zohar. “Accelerating Bitcoin’s Transaction Processing. Fast Money Grows on Trees, Not Chains.” In: *IACR Cryptology ePrint Archive* 2013.881 (2013).

[19] Friedhelm Victor and Bianca Katharina Lüders. “Measuring ethereum-based erc20 token networks”. In: *International Conference on Financial Cryptography and Data Security*. 2019.

[20] Solidity. *"Docs-Solidity"*. URL: `https://solidity.readthedocs.io/en/v0.5.3/index.html#` (visited on 10/03/2019).

[21] Web3js. *"Docs-Web3.js"*. URL: `https://web3js.readthedocs.io/en/v1.2.1/index.html` (visited on 10/04/2019).

[22] P Golda Jeyasheeli and L Rajashree. “Cost effective file replication in P2P file sharing systems”. In: *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*. IEEE. 2012, pp. 948–952.

[23] LLC. Muvi®. *Muvi - Pricing*. Tech. rep. 18th December, 2018.

# PHỤ LỤC

**Code tham khảo hàm băm SHA-256**

```
function [digest, MSG_RAW_512] = hash(LEN,METH,GEN)

SHA256=1;

 PAD_ZERO=64;
 MFACT=1;
 MSG_SZ_P_BLK=512*MFACT;
 MOD_SZ_BLK  = 448*MFACT;
KT=[
'428a2f98'; '71374491'; 'b5c0fbcf'; 'e9b5dba5'; '3956c25b'; '59f111f1';
'd807aa98'; '12835b01'; '243185be'; '550c7dc3'; '72be5d74'; '80deb1fe';
'e49b69c1'; 'efbe4786'; '0fc19dc6'; '240ca1cc'; '2de92c6f'; '4a7484aa';
'983e5152'; 'a831c66d'; 'b00327c8'; 'bf597fc7'; 'c6e00bf3'; 'd5a79147';
'27b70a85'; '2e1b2138'; '4d2c6dfc'; '53380d13'; '650a7354'; '766a0abb';
'a2bfe8a1'; 'a81a664b'; 'c24b8b70'; 'c76c51a3'; 'd192e819'; 'd6990624';
'19a4c116'; '1e376c08'; '2748774c'; '34b0bcb5'; '391c0cb3'; '4ed8aa4a';
'748f82ee'; '78a5636f'; '84c87814'; '8cc70208'; '90befffa'; 'a4506ceb';

h0 = dec2bin(hex2dec('6a09e667'),32); disp(h0);
h1 = dec2bin(hex2dec('bb67ae85'),32); disp(h1);
h2 = dec2bin(hex2dec('3c6ef372'),32); disp(h2);
h3 = dec2bin(hex2dec('a54ff53a'),32);
h4 = dec2bin(hex2dec('510e527f'),32);
h5 = dec2bin(hex2dec('9b05688c'),32);
h6 = dec2bin(hex2dec('1f83d9ab'),32);
h7 = dec2bin(hex2dec('5be0cd19'),32);

INV_M  =dec2bin(hex2dec('FFFFFFFF'), 32); disp(INV_M);
INV_M64=num2str(ones(64,1))'; disp(INV_M64);
```

```
%%
if LEN < 0
    disp ('--- EXIT STATUS: Invalid MESG LENGTH ENTERED---');
    disp (' RE-ENTER MESG LENGTH, valid entries are 0-512' );
    disp ('-------------------------------------');
    return
elseif(LEN>=1)
    mesg_d=((sign(rand(1,LEN)-0.5)) + 1) *0.5;
    for u=1:LEN
        mesg_d(u)=mod(u,2);
    end
end
%%
if(GEN==1)
    msg_str=char();
    k=0;
    if(LEN>0)
        for i=1:length(mesg_d),
            msg_str = strcat(msg_str,num2str(mesg_d(i))) ;
        end
    end
end
%%
MSG_RAW_512=char();
raw_str=char();
raw_str=msg_str;
blk_num = fix(length(msg_str)/(512*MFACT)) ;
if(mod(length(msg_str),(512*MFACT)) ==0)
    blk_num = blk_num -1;
end
if(blk_num<0)
   blk_num=0;
end
```

```
extnd=512*MFACT*(blk_num+1)-mod(length(msg_str),(512*MFACT));
raw_str(end+1:end+extnd)= num2str(round(rand(1,extnd))')';

for k=1:128*(blk_num+1)*MFACT
    MSG_RAW_512 = strcat(MSG_RAW_512,dec2hex(bin2dec(
    raw_str(4*(k-1)+1:4*k))));
end
 %%
msg_str(end+1) = '1';
int_k=0;
diff_k = abs(int_k+LEN+1-448*MFACT);
while(mod(diff_k,512*MFACT) ~=0)
    int_k  = int_k +1;
    diff_k = abs(int_k+LEN+1-448*MFACT);
end
k=int_k;
tpr=sprintf('Min. K satisfying l+k+1 = %d mod %d is %d ',
MOD_SZ_BLK, MSG_SZ_P_BLK,k);
msg_str(end+1:end+k)='0'; %% Pad K-bits of '0's
len_bits=dec2bin(LEN,PAD_ZERO); %% 64-bit representation of MSG_LEN
MSG_2_PROC=cat(2,msg_str,len_bits); %%MESG after PreProcess
MSG_PADDED=char();
no_512_blk=length(MSG_2_PROC)/MSG_SZ_P_BLK;
for k=1:(128*MFACT)*(no_512_blk)
    MSG_PADDED = strcat(MSG_PADDED,dec2hex(bin2dec(
    MSG_2_PROC(4*(k-1)+1:4*k))));
end
MSG_L = length(MSG_2_PROC);
N=0;
if (mod(MSG_L,512*MFACT) == 0)
    N=MSG_L/(512*MFACT);
    tprint=sprintf('No. of %d-bit MESG chunks=%d', MSG_SZ_P_BLK, N);
else
```

```
    disp('Error in MESG PreProcessing');
    disp('Check');
return
end
%% Process MSG BLKs
for blk_num=1:N
    padded_msg=MSG_2_PROC(
    (512*MFACT*(blk_num-1)+1):blk_num*512*MFACT);

    %% Parse MESG WORDs
    for i=1:16,
        for q=1:32
            W(i,q)=str2num(padded_msg(32*(i-1)+q));
        end
    end
    for i=17:64

        tmp1=W(i-2,:);
        tmp_ror= cat(2,tmp1(end-16:end),tmp1);
        ror_17 = tmp_ror(1:32);
        tmp_ror= cat(2,tmp1(end-18:end),tmp1);
        ror_19 = tmp_ror(1:32);
        tmp_sh= cat(2,tmp1(end-9:end),tmp1);
        shr_10  = tmp_sh(1:32);
        shr_10(1,[1:10])=0;
        tmpx1  = bitxor(ror_17, ror_19);
        sigma1 = bitxor(shr_10,tmpx1);

        tmp1=W(i-15,:);
        tmp_ror = cat(2,tmp1(end-6:end),tmp1);
        ror_7   = tmp_ror(1:32);
        tmp_ror = cat(2,tmp1(end-17:end),tmp1);
        ror_18  = tmp_ror(1:32);
```

```
        tmp_sh   = cat(2,tmp1(end-2:end),tmp1);
        shr_3    = tmp_sh(1:32);
        shr_3(1,[1:3])=0;
        tmpx1    = bitxor(ror_7, ror_18);
        sigma0   = bitxor(shr_3, tmpx1);
        tmp_add = mod((bin2dec(
        num2str(sigma1')') + bin2dec(num2str(sigma0')') + bin2dec(
        num2str((W(i-7,:))')') + bin2dec(
        num2str((W(i-16,:))')')),4294967296);
       W(i,:)   = str2num(dec2bin(tmp_add,32)')';
    end
     for j=1:32
            a(j)=str2num(h0(j));
            b(j)=str2num(h1(j));
            c(j)=str2num(h2(j));
            d(j)=str2num(h3(j));
            e(j)=str2num(h4(j));
            f(j)=str2num(h5(j));
            g(j)=str2num(h6(j));
            h(j)=str2num(h7(j));
            bitmask(j)=str2num(INV_M(j));
     end
    for i=1:64

           ror_6   = cat(2, e(end-5:end),e);
           ror_6=ror_6(1:32);
           ror_11  = cat(2, e(end-10:end),e);ror_11=ror_11(1:32);
           ror_25  = cat(2, e(end-24:end),e);ror_25=ror_25(1:32);
           tmp_ror = bitxor(ror_6, ror_11);
           S_SIG1  = bitxor(tmp_ror, ror_25);
           not_e   = bitxor(e,bitmask);
           and_ef  = bitand(e,f);
           and_fg  = bitand(not_e,g);
```

```
ch_efg   = bitxor(and_ef, and_fg);
add_t1   = mod((bin2dec(num2str(h')') + bin2dec(
num2str(S_SIG1')') + bin2dec(
num2str(ch_efg')') + hex2dec(KT(i,:)) + bin2dec(
num2str(W(i,:)')')), 4294967296) ;

ror_2  = cat(2, a(end-1:end),a);
ror_2  = ror_2(1:32);
ror_13 = cat(2, a(end-12:end),a);
ror_13 = ror_13(1:32);
ror_22 = cat(2, a(end-21:end),a);
ror_22 = ror_22(1:32);
tmp_ror = bitxor(ror_2, ror_13);
S_SIG0  = bitxor(tmp_ror, ror_22);
and_ab  = bitand(a,b);
and_bc  = bitand(b,c);
and_ac  = bitand(a,c);
xor_ab_bc = bitxor(and_ab,and_bc);

maj_abc = bitxor(xor_ab_bc,and_ac);

add_t2  = mod((bin2dec(num2str(maj_abc')') +  bin2dec(
num2str(S_SIG0')')), 4294967296);
h=g;
g=f;
f=e;
int_e= mod((bin2dec(num2str(d')')+add_t1),4294967296 );
numd=dec2bin(int_e,32);
for z=1:32
   e(z)=str2num(numd(z));
end
d=c;
c=b;
```

```
        b=a;
        int_a=mod((add_t1 + add_t2), 4294967296);
        numd=dec2bin(int_a ,32);
        for z=1:32
          a(z)=str2num(numd(z));
        end
    end
    h0_dec = mod(bin2dec(h0) + bin2dec(num2str(a')'), 4294967296);
    h1_dec = mod(bin2dec(h1) + bin2dec(num2str(b')'), 4294967296);
    h2_dec = mod(bin2dec(h2) + bin2dec(num2str(c')'), 4294967296);
    h3_dec = mod(bin2dec(h3) + bin2dec(num2str(d')'), 4294967296);
    h4_dec = mod(bin2dec(h4) + bin2dec(num2str(e')'), 4294967296);
    h5_dec = mod(bin2dec(h5) + bin2dec(num2str(f')'), 4294967296);
    h6_dec = mod(bin2dec(h6) + bin2dec(num2str(g')'), 4294967296);
    h7_dec = mod(bin2dec(h7) + bin2dec(num2str(h')'), 4294967296);

    h0 = dec2bin(h0_dec,32);
    h1 = dec2bin(h1_dec,32);
    h2 = dec2bin(h2_dec,32);
    h3 = dec2bin(h3_dec,32);
    h4 = dec2bin(h4_dec,32);
    h5 = dec2bin(h5_dec,32);
    h6 = dec2bin(h6_dec,32);
    h7 = dec2bin(h7_dec,32);

    H0 = (dec2hex(h0_dec,8));
    H1 = (dec2hex(h1_dec,8));
    H2 = (dec2hex(h2_dec,8));
    H3 = (dec2hex(h3_dec,8));
    H4 = (dec2hex(h4_dec,8));
    H5 = (dec2hex(h5_dec,8));
    H6 = (dec2hex(h6_dec,8));
    H7 = (dec2hex(h7_dec,8));
```

```
    digest = char();
    digest = strcat(H0,H1,H2,H3,H4, H5,H6, H7);
end

tsc=sprintf('++++HASH generated using ALgorithm %s = %s', METH, digest);
disp(tsc);
return
```

**Code tham khảo Smart Contract**

```
pragma solidity ^0.5.0;
pragma experimental ABIEncoderV2;
contract SimpleStorage1 {
    string[] storedData;
    string[] storedData1;
    address[] storedData2;

    constructor() public payable{

    }
    function() payable external {}
    function set(string memory x, string memory y, address z) public {
        storedData.push(x);
        storedData1.push(y);
        storedData2.push(z);
    }

    function get() public view returns (string[] memory, string[] memor
        return (storedData, storedData1, storedData2);
    }
    function length() public view returns (uint)
    {
        return storedData.length;
```

```
    }
    mapping(address => uint) public count;
    function upVote(address x) public
    {
        count[x] ++;
    }
    function getUpVote(address x) public view returns (uint){
        return count[x];
    }
    function grant(address payable x) public
    {
        x.transfer(1 ether);
    }
    function getBalance() public view returns (uint256) {
        return address(this).balance;
    }
}
```